Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Release 5.2(6)

Release Date: August 09, 2012

Part Number: OL-27554-01 J0

This document describes the caveats and limitations for switches in the Cisco MDS 9000 Family. Use this document in conjunction with documents listed in the "Related Documentation" section on page 62.

Release notes are sometimes updated with new information on restrictions and caveats. Refer to the following website for the most recent version of the *Cisco MDS 9000 Family Release Notes*: http://www.cisco.com/en/US/products/ps5989/prod_release_notes_list.html

Table 1 shows the on-line change history for this document.

Table 1 Online History Change

Revision	Date	Description
A0	August 09, 2012	Created the release notes.
B0	August 29, 2012	Added M91S2K9-5.2.6 for the MDS 9134 and the MDS 9124 switches to Table 2.
C0	September 11, 2012	Updated the guidelines for smart zoning in the "Smart Zoning" section.
D0	September 20, 2012	Added an explanation of a syntax error to the "Downgrading Guidelines Specific to NX-OS Release 5.2(6)" section.
E0	September 28, 2012	Updated the"Deprecated Features" section.
F0	October 08, 2012	Added open caveat CSCuc35483.
G0	November 8, 2012	Added the "NPE Software Images" section.
H0	February 13, 2013	Updated the "New Features in Cisco MDS NX-OS Release 5.2" section to include new features from earlier 5.2 releases.
I0	March 12, 2013	Added open caveat CSCuc84790.
J0	April 5, 2013	Added open caveat CSCuf31077.
K0	August 13, 2013	Add ed open caveat CSCuh27347.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Table 1 Online History Change

Revision	Date	Description
K0	May 31, 2013	Added resolved caveat CSCtr01652.
L0	June 13	Added open caveat CSCub47799.
M0	Sept 15, 2014	Added open caveat CSCtz53329.

Contents

This document includes the following:

- Introduction, page 2
- Components Supported, page 2
- MDS 9000 Chassis and Module Support, page 9
- Software Download Process, page 13
- Upgrading Your Cisco MDS NX-OS Software Image, page 16
- Downgrading Your Cisco MDS SAN-OS Software Image, page 20
- Licensed Cisco NX-OS Software Packages, page 29
- Licensed Cisco NX-OS Software Packages, page 29
- Deprecated Features, page 31
- Limitations and Restrictions, page 32
- Caveats, page 39
- Related Documentation, page 62
- Obtaining Documentation and Submitting a Service Request, page 64

Introduction

The Cisco MDS 9000 Family of Multilayer Directors and Fabric Switches provides industry-leading availability, scalability, security, and management, allowing you to deploy high performance storage-area networks with lowest total cost of ownership. Layering a rich set of intelligent features onto a high-performance, protocol-agnostic switch fabric, the Cisco MDS 9000 Family addresses the stringent requirements of large data center storage environments: uncompromising high availability, security, scalability, ease of management, and seamless integration of new technologies.

Cisco MDS 9000 NX-OS software powers the award-winning Cisco MDS 9000 Series Multilayer Switches. It is designed to create a strategic SAN platform with superior reliability, performance, scalability, and features. Formerly known as Cisco SAN-OS, Cisco MDS 9000 NX-OS software is fully interoperable with earlier Cisco SAN-OS versions and enhances hardware platform and module support.

Components Supported

Table 2 lists the NX-OS software part numbers and hardware components supported by the Cisco MDS 9000 Family.

Note For the latest information about supported transceivers, see the *Cisco MDS 9000 Family Pluggable Transceivers* data sheet.

Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components

Component	Part Number	Description	Applicable Product
Software	M95S2K9-5.2.6	MDS 9500 Supervisor/Fabric-2, NX-OS software	MDS 9500 Series only
	M92S2K9-5.2.6	MDS 9200 Supervisor/Fabric-2, NX-OS software	MDS 9222i Switch only
	M91S3K9-5.2.6	MDS 9148 Supervisor/Fabric-3 NX-OS software	MDS 9148 Switch
	M91S2K9-5.2.6	MDS 9100 Supervisor/Fabric-2, NX-OS software	MDS 9134 Switch and MDS 9124 Switch

Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
Licenses	M9500SSE184K9	Storage Services Enabler License for one MSM-18/4 module	MDS 9500 Series only
	M9222ISSE1K9	Storage Services Enabler License	MDS 9222i Switch only
	M9200SSE184K9	Storage Services Enabler License for one MSM-18/4 module	MDS 9200 Series only
	M95DMM184K9	Data Mobility Manager License for one MSM-18/4 module	MDS 9500 Series only
	M9222IDMMK9	Data Mobility Manager License for Cisco MDS 9222i	MDS 9222i Switch
	M92DMM184K9	Data Mobility Manager License for one MSM-18/4 module	MDS 9200 Series only
	M95DMM184TSK9	Data Mobility Manager for one MSM-18/4 module — Time Limited to 180 days only	MDS 9500 Series only
	M9222IDMMTSK9	Data Mobility Manager — Time Limited to 180 days only	MDS 9222i Switch only
	M92DMM184TSK9	Data Mobility Manager for one MSM-18/4 module — Time Limited to 180 days only	MDS 9200 Series only
	M92SSESSNK9	Cisco Storage Services Enabler License for SSN-16 (1 engine)	MDS 9200 Series only
	M95SSESSNK9	Cisco Storage Services Enabler License for SSN-16 (1 engine)	MDS 9500 Series only
	M92SMESSNK9	Cisco Storage Media Encryption License for SSN-16 (1 engine)	MDS 9200 Series only
	M95SMESSNK9	Cisco Storage Media Encryption License for SSN-16 (1 engine)	MDS 9500 Series only
	M92IOASSN	Cisco I/O Accelerator License for SSN-16 (1 engine)	MDS 9200 Series only
	M95IOASSN	Cisco I/O Accelerator License for SSN-16 (1 engine)	MDS 9500 Series only
	M92IOA184	Cisco I/O Accelerator License for MSM-18/4	MDS 9200 Series only
	M95IOA184	Cisco I/O Accelerator License for MSM-18/4	MDS 9500 Series only
	M9222IIOA	Cisco I/O Accelerator License for Cisco MDS 9222i base switch	MDS 9222i Switch only
	M92EXTSSNK9	Cisco SAN Extension License for SSN-16 (1 engine)	MDS 9200 Series only
	M95EXTSSNK9	Cisco SAN Extension License for SSN-16 (1 engine)	MDS 9500 Series only
	M9200XRC	Cisco XRC Acceleration	MDS 9200 Series only
	M9500XRC	Cisco XRC Acceleration	MDS 9500 Series only

Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
Chassis	DS-C9513	Cisco MDS 9513 Multilayer Director (13-slot multilayer director with 2 slots for Supervisor-2 modules, with 11 slots available for switching modules — SFPs sold separately)	MDS 9513 Switch
	DS-C9509	Cisco MDS 9509 Multilayer Director (9-slot multilayer director with 2 slots for Supervisor modules, with 7 slots available for switching modules — SFPs sold separately)	MDS 9509 Switch
	DS-C9506	Cisco MDS 9506 Multilayer Director (6-slot multilayer director with 2 slots for Supervisor modules, with 4 slots available for switching modules — SFPs sold separately)	MDS 9506 Switch
	DS-C9222i-K9	Cisco MDS 9222i Multilayer Fabric Switch (3-rack-unit (3RU) semimodular multilayer fabric switch with 18 4-Gbps Fibre Channel ports, 4 Gigabit Ethernet ports, and a modular expansion slot for Cisco MDS 9000 Family Switching and Services modules)	MDS 9222i Switch
	DS-C9148-K9	Cisco MDS 9148 48-Port Multilayer Fabric Switch (1RU fixed-configuration multilayer fabric switch with 48 8-Gbps Fibre Channel ports)	MDS 9148 Switch
	DS-C9134-K9	Cisco MDS 9134 34-Port Multilayer Fabric Switch (1RU fixed-configuration multilayer fabric switch with 32 4-Gbps and 2 10-Gbps Fibre Channel ports)	MDS 9134 Switch
	DS-C9124-K9	Cisco MDS 9124 24-Port Multilayer Fabric Switch (1RU fixed-configuration multilayer fabric switch with 24 4-Gbps Fibre Channel ports)	MDS 9124 Switch
Supervisor Modules	DS-X9530-SF2-K9	Cisco MDS 9500 Series Supervisor-2 Module	MDS 9500 Series
	DS-X9530-SF2A-K9	Cisco MDS 9500 Series Supervisor-2A Module	MDS 9500 Series

Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
Switching Modules	DS-X9112	Cisco MDS 9000 12-port 4-Gbps Fibre Channel Switching Module with SFP LC connectors	MDS 9500 Series MDS 9200 Series
	DS-X9124	Cisco 24-port 4-Gbps Fibre Channel Switching Module with SFP LC connectors	MDS 9500 Series MDS 9200 Series
	DS-X9148	Cisco MDS 9000 48-port 4-Gbps Fibre Channel Switching Module with SFP LC	MDS 9500 Series MdS 9200 Series
	DS-X9704	Cisco MDS 9000 Family 4-Port 10-Gbps Fibre Channel Switching Module with SFP LC	MDS 9500 Series MDS 9200 Series
	DS-X9224-96K9	Cisco MDS 9000 24-Port 8-Gbps Fibre Channel Switching Module with SFP and SFP+ LC connectors	MDS 9500 Series
	DS-X9248-96K9	Cisco MDS 9000 48-Port 8-Gbps Fibre Channel Switching Module with SFP and SFP+ LC connectors	MDS 9500 Series
	DS-X9248-48K9	Cisco MDS 9000 4/44-Port Host-Optimized 8-Gbps Fibre Channel Switching Module with SFP and SFP+ LC connectors	MDS 9500 Series MDS 9222i Switch
	DS-X9708-K9	Cisco MDS 9000 8-port 10-Gbps Fibre Channel over Ethernet (FCoE) Module	MDS 9500 Series
	DS-X9232-256K9	Cisco MDS 9000 32-port 8-Gbps Advanced Fibre Channel Switching Module	MDS 9500 Series
	DS-X9248-256K9	Cisco MDS 9000 48-port 8-Gbps Advanced Fibre Channel Switching Module	MDS 9500 Series
Services Modules	DS-X9316-SSNK9	Cisco MDS 9000 Family 16-Port Storage Services Node (SSN-16) — 16 fixed 1-Gbps Ethernet ports, plus 4 service engines that support 16 Gigabit Ethernet IP storage services ports.	MDS 9500 Series MDS 9222i Switch
	DS-X9304-18K9	Cisco MDS 9000 18/4-Port Multiservice Module (MSM-18/4) — 18-port, 4-Gbps Fibre Channel plus 4-port Gigabit Ethernet IP services and switching module with SFP LC connectors	MDS 9500 Series MDS 9200 Series
External crossbar module	DS-13SLT-FAB1	Cisco MDS 9513 Switching Fabric 1 Module	MDS 9513 Switch
	DS-13SLT-FAB2	Cisco MDS 9513 Switching Fabric 2 Module	MDS 9513 Switch
	DS-13SLT-FAB3	Cisco MDS 9513 Switching Fabric 3 Module	MDS 9513 Switch

Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
Optics	SFP-10G-SR	10GBASE-SR SFP+ Module	MDS 9500 Series, 8-port 10-Gbps FCoE Module (DS-X9708-K9)
	SFP-10G-LR	10GBASE-LR SFP+ Module	MDS 9500 Series, 8-port 10-Gbps FCoE Module (DS-X9708-K9)
	SFP-H10GB-CU1M	10GBASE-CU SFP+ cable 1 meter	MDS 9500 Series, 8-port 10-Gbps FCoE Module (DS-X9708-K9)
	SFP-H10GB-CU3M	10GBASE-CU SFP+ cable 3 meter	MDS 9500 Series, 8-port 10-Gbps FCoE Module (DS-X9708-K9)
	SFP-H10GB-CU5M	10GBASE-CU SFP+ cable 5 meter	MDS 9500 Series, 8-port 10-Gbps FCoE Module (DS-X9708-K9)
	SFP-H10GB-ACU7M	10GBASE-CU SFP+ active copper cable 7 meter	MDS 9500 Series, 8-port 10-Gbps FCoE Module (DS-X9708-K9)
	SFP-H10GB-ACU10M	10GBASE-CU SFP+ active copper cable 10 meter	MDS 9500 Series, 8-port 10-Gbps FCoE Module (DS-X9708-K9)

Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
LC-type fiber-optic SFP	DS-FC10G-SW	SFP+ optics (LC type) for 10-Gbps Fibre Channel for shortwave mode	32-port 8-Gbps Advanced Fibre Channel Module (DS-X9232-256K9), 48-port 8-Gbps Advanced Fibre Channel Module (DS-X9248-256-K9)
	DS-FC10G-LW	SFP+ optics (LC type) for 10-Gbps Fibre Channel for longwave mode	32-port 8-Gbps Advanced Fibre Channel Module (DS-X9232-256K9), 48-port 8-Gbps Advanced Fibre Channel Module (DS-X9248-256-K9)
	DS-SFP-FC8G-ER	SFP+ optics (LC type) for 2-, 4-, or 8-Gbps Fibre Channel for extended reach (40 km reach)	MDS DS-X9200 Series switching modules, MDS 9148
	DS-SFP-FC8G-SW	SFP+ optics (LC type) for 2-, 4-, or 8-Gbps Fibre Channel for shortwave mode	MDS DS-X9200 Series switching modules
	DS-SFP-FC8G-LW	SFP+ optics (LC type) for 2-, 4-, or 8-Gbps Fibre Channel for longwave mode; supports distances up to 10 km	MDS DS-X9200 Series switching modules
	DS-SFP-FC4G-SW	SFP optics (LC type) for 1-, 2-, or 4-Gbps Fibre Channel for shortwave mode	MDS 9124, MDS 9134, MDS 9148, MDS 9222i, DS-X9100, and DS-X9200 Series switching modules
	DS-SFP-FC4G-MR	SFP optics (LC type) for 1-, 2-, or 4-Gbps Fibre Channel for longwave mode; supports distances up to 4 km	MDS 9124, MDS 9134, MDS 9222i, DS-X9100, and DS-X9200 Series switching modules
	DS-SFP-FC4G-LW	SFP optics (LC type) for 1-, 2-, or 4-Gbps Fibre Channel for longwave mode; supports distances up to 10 km	MDS 9124, MDS 9134, MDS 9222i, DS-X9100, and DS-X9200 Series switching modules
	DS-SFP-FCGE-SW	SFP optics (LC type) for 1-Gbps Ethernet and 1- or 2-Gbps Fibre Channel for shortwave mode; not supported for use in 4-Gbps-capable ports	MDS 9000 Series
	DS-SFP-FCGE-LW	SFP optics (LC type) for 1-Gbps Ethernet and 1- or 2-Gbps Fibre Channel for longwave mode; not supported for use in 4-Gbps-capable ports	MDS 9000 Series
	DS-SFP-GE-T	SFP (RJ-45 connector) for Gigabit Ethernet over copper	MDS 9000 Series
Cisco Coarse Wavelength - Division Multiplexing (CWDM)	DS-CWDM-xxxx	CWDM Gigabit Ethernet and 1- or 2-Gbps Fibre Channel SFP LC type, where product number xxxx = 1470, 1490, 1510, 1530, 1550, 1570, 1590, or 1610 nm	MDS 9000 Family
	DS-CWDM4Gxxxx	CWDM 4-Gbps Fibre Channel SFP LC type, where product number xxxx = 1470, 1490, 1510, 1530, 1550, 1570, 1590, or 1610 nm	MDS 9000 Family

Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
Dense Wavelength - Division Multiplexing (DWDM)	DWDM-X2-xx.xx	DWDM X2 SC optics for 10-Gbps Fibre Channel connectivity to an existing Ethernet DWDM infrastructure, with 15xx.xx nm wavelength, where xx.xx = 60.61, 59.79, 58.98, 58.17, 56.55, 55.75, 54.94, 54.13, 52.52, 51.72, 50.92, 50.12, 48.51, 47.72, 46.92, 46.12, 44.53, 43.73, 42.94, 42.14, 40.56, 39.77, 38.98, 38.19, 36.61, 35.82, 35.04, 34.25, 32.68, 31.90, 31.12, or 30.33	MDS 9500 Series MDS 9200 Series
	DWDM-SFP-xxxx	DWDM Gigabit Ethernet and 1- or 2-Gbps Fibre Channel SFP LC type, where product number xxxx = 3033, 3112, 3190, 3268, 3425, 3504, 3582, 3661, 3819, 3898, 3977, 4056, 4214, 4294, 4373, 4453, 4612, 4692, 4772, 4851, 5012, 5092, 5172, 5252, 5413, 5494, 5575, 5655, 5817, 5898, 5979, or 6061nm	MDS 9000 Family
Add/Drop Multiplexer (ADM)	DS-CWDMOADM4A	4-channel CWDM optical ADM (OADM) module (Cisco CWDM 1470, 1490, 1510, or 1530 NM Add/Drop Module)	MDS 9000 Family
	DS-CWDMOADM4B	4-channel CWDM OADM module (Cisco CWDM 1550, 1570, 1590, or 1610 NM Add/Drop Module)	MDS 9000 Family
	DS-CWDM-MUX8A	ADM for 8 CWDM wavelengths	MDS 9000 Family
CWDM Multiplexer Chassis	DS-CWDMCHASSIS	2-slot chassis for CWDM ADMs	MDS 9000 Family
Power Supplies	DS-CAC-300W	300W AC power supply	MDS 9100 Series
	DS-C24-300AC	300W AC power supply	MDS 9124 Switch
	DS-CAC-845W	845W AC power supply for Cisco MDS 9200 Series	MDS9200 Series
	DS-CAC-3000W	3000W AC power supply for Cisco MDS 9509	MDS 9509 Switch
	DS-CAC-2500W	2500W AC power supply	MDS 9509 Switch
	DS-CDC-2500W	2500W DC power supply	MDS 9509 Switch
	DS-CAC-6000W	6000W AC power supply for Cisco MDS 9513	MDS 9513 Switch
	DS-CAC-1900W	1900W AC power supply for Cisco MDS 9506	MDS 9506 Switch
CompactFlash	MEM-MDS-FLD512M	External 512-MB CompactFlash memory for supervisor module	MDS 9500 Series
Port Analyzer Adapter	DS-PAA-2, DS-PAA	A standalone Fibre Channel-to-Ethernet adapter that allows for simple, transparent analysis of Fibre Channel traffic in a switched fabric	MDS 9000 Family
Smart Card Reader	DS-SCR-K9	Storage Media Encryption (SME) Smart Card Reader	MDS 9000 Family
Smart Card	DS-SC-K9	SME Smart Card	MDS 9000 Family

MDS 9000 Chassis and Module Support

Table 3 lists the MDS hardware chassis supported by Cisco MDS NX-OS 5.x.

Table 3 Cisco MDS NX-OS 5.x Chassis Support Matrix

Switch	NX-OS 5.x Support
MDS 9513	Yes
MDS 9509	Yes
MDS 9506	Yes
MDS 9222i	Yes
MDS 9148	Yes
Cisco MDS 8-Gb Fabric Switch for HP c-Class Blade System	Yes
MDS 9134	Yes[1]
MDS 9124	Yes[1]
Cisco MDS 4-Gbps Fabric Switch for HP c-Class BladeSystem	Yes[1]
Cisco MDS 4-Gbps Fabric Switch for IBM BladeCenter	Yes[1]

1. This switch supports Cisco MDS NX-OS Release 5.2(2) and later releases, but does not support Release 5.2(1).

Table 4 lists the MDS hardware modules supported by Cisco MDS NX-OS 5.x. For the list of MDS hardware modules supported by Cisco MDS SAN-OS 4.x, see Table 5. For the list of MDS hardware modules supported by Cisco MDS SAN-OS 3.x, see Table 6.

Table 4 Module Support Matrix for Cisco MDS NX-OS 5.x

Module	Description	MDS 9500 Series		MDS 9222i	
		NX-OS 5.2(x)	NX-OS 5.0(x)	NX-OS 5.2(x)	NX-OS 5.0(x)
DS-X9530-SF2-K9	MDS 9500 Supervisor-2 Module	Yes	Yes	N/A	N/A
DS-X9530-SF2A-K9	MDS 9500 Supervisor-2A Module	Yes	Yes	N/A	N/A
DS-13SLT-FAB3	MDS 9513 Fabric Module 3	Yes	No	N/A	N/A
DS-13SLT-FAB2	MDS 9513 Fabric Module 2	Yes	Yes	N/A	N/A
DS-13SLT-FAB1	MDS 9513 Fabric Module 1	Yes	Yes	N/A	N/A
DS-X9708-K9	8-port 10-Gbps FCoE Module	Yes[1,2]	No	No	No
DS-X9232-256K9	32-port 8-Gbps Advanced Fibre Channel Switching Module	Yes[1]	No	No	No
DS-X9248-256K9	48-port 8-Gbps Advanced Fibre Channel Switching Module	Yes[1]	No	No	No
DS-X9224-96K9	24-port 8-Gbps Fibre Channel Switching Module	Yes[1]	Yes[3]	No	No
DS-X9248-96K9	48-port 8-Gbps Fibre Channel Switching Module	Yes[1]	Yes[3]	No	No
DS-X9248-48K9	4/44-port Host Optimized 8-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes

Table 4 Module Support Matrix for Cisco MDS NX-OS 5.x (continued)

Module	Description	MDS 9500 Series		MDS 9222i	
		NX-OS 5.2(x)	NX-OS 5.0(x)	NX-OS 5.2(x)	NX-OS 5.0(x)
DS-X9316-SSNK9	16-port Storage Services Node (SSN-16)	Yes	Yes	Yes	Yes
DS-X9304-18K9	18/4-Port Multiservice Module (MSM-18/4)	Yes	Yes	Yes	Yes
DS-X9112	12-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes
DS-X9124	24-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes
DS-X9148	48-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes
DS-X9704	4-port 10-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes

1. Requires DS-13SLT-FAB3 or DS-13SLT-FAB2 in the MDS 9513.
2. Requires the Supervisor-2A module.
3. Requires DS-13SLT-FAB2 in the MDS 9513.

Table 5 Module Support Matrix for Cisco MDS NX-OS 4.x

Module	Description	MDS 9500 Series	MDS 9222i	MDS 9216i
DS-X9530-SF2-K9	MDS 9500 Supervisor-2 Module	Yes	N/A	N/A
DS-X9530-SF2A-K9	MDS 9500 Supervisor-2A Module	Yes[1]	N/A	N/A
DS-X9530-SF1-K9	MDS 9500 Supervisor-1 Module	No	N/A	N/A
DS-13SLT-FAB2	MDS 9513 Fabric Module 2	Yes	N/A	N/A
DS-13SLT-FAB1	MDS 9513 Fabric Module 1	Yes	N/A	N/A
DS-X9224-96K9	24-port 8-Gbps Fibre Channel Switching Module	Yes[2]	No	No
DS-X9248-96K9	48-port 8-Gbps Fibre Channel Switching Module	Yes[2]	No	No
DS-X9248-48K9	4/44-port Host Optimized8-Gbps Fibre Channel Switching Module	Yes	Yes	No
DS-X9316-SSNK9	16-port Storage Services Node (SSN-16)	Yes	Yes	Yes
DS-X9304-18K9	18/4-Port Multiservice Module (MSM-18/4)	Yes	Yes	Yes
DS-X9112	12-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes
DS-X9124	24-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes
DS-X9148	48-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes
DS-X9704	4-port 10-Gbps Fibre Channel Switching Module	Yes	Yes	Yes
DS-X9302-14K9	14/2-port Multiprotocol Services (MPS-14/2) Module	Yes	No	Yes
DS-X9016	16-port 1-, 2-Gbps Fibre Channel Switching Module	Yes	No	Yes

Table 5 Module Support Matrix for Cisco MDS NX-OS 4.x (continued)

Module	Description	MDS 9500 Series	MDS 9222i	MDS 9216i
DS-X9032	32-port 1-, 2-Gbps Fibre Channel Switching Module	Yes	No	Yes
DS-X9032-SSM	32-port Storage Services Module (SSM)	Yes	Yes	Yes
DS-X9308-SMIP	8-port 1-, 2-Gbps IP Switching Module	No	No	No
DS-X9304-SMIP	4-port 1-, 2-Gbps IP Switching Module	No	No	No

1. In software releases earlier than Cisco NX-OS Release 4.2(7a), the Supervisor-2A module appears as unsupported hardware in Device Manager, but the Supervisor-2A module does work with Cisco NX-OS release 4.x software.
2. Requires DS-13SLT-FAB2 in the MDS 9513.

Table 6 lists the MDS hardware modules supported by Cisco MDS SAN-OS 3.x.

Table 6 Module Support Matrix for Cisco MDS SAN-OS 3.x

Module	Description	MDS 9500 Series	MDS 9222i	MDS 9216i	MDS 9216A	MDS 9216
DS-X9530-SF2-K9	MDS 9500 Supervisor-2 Module	Yes	N/A	N/A	N/A	N/A
DS-X9530-SF2A-K9	MDS 9500 Supervisor-2A Module	Yes[1]	N/A	N/A	N/A	N/A
DS-X9530-SF1-K9	MDS 9500 Supervisor-1 Module	Yes	N/A	N/A	N/A	N/A
DS-13SLT-FAB2	MDS 9513 Fabric Module 2	Yes	N/A	N/A	N/A	N/A
DS-13SLT-FAB1	MDS 9513 Fabric Module 1	Yes	N/A	N/A	N/A	N/A
DS-X9224-96K9	24-port 8-Gbps Fibre Channel Switching Module	No	No	No	No	No
DS-X9248-96K9	48-port 8-Gbps Fibre Channel Switching Module	No	No	No	No	No
DS-X9248-48K9	4/44-port Host Optimized8-Gbps Fibre Channel Switching Module	No	No	No	No	No
DS-X9316-SSNK9	16-port Storage Services Node (SSN-16)	No	No	No	No	No
DS-X9304-18K9	18/4-Port Multiservice Module (MSM-18/4)[2]	Yes	Yes	Yes	Yes	No
DS-X9112	12-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes	No
DS-X9124	24-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes	No
DS-X9148	48-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes	No
DS-X9704	4-port 10-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes	No
DS-X9302-14K9	14/2-port Multiprotocol Services (MPS-14/2) Module	Yes	No	Yes	Yes	Yes
DS-X9016	16-port 1-, 2-Gbps Fibre Channel Switching Module	Yes	No	Yes	Yes	Yes

Table 6 Module Support Matrix for Cisco MDS SAN-OS 3.x (continued)

Module	Description	MDS 9500 Series	MDS 9222i	MDS 9216i	MDS 9216A	MDS 9216
DS-X9032	32-port 1-, 2-Gbps Fibre Channel Switching Module	Yes	No	Yes	Yes	Yes
DS-X9032-SSM	32-port Storage Services Module (SSM)	Yes	Yes	Yes	Yes	Yes
DS-X9308-SMIP	8-port 1-, 2-Gbps IP Switching Module	Yes	No	Yes	Yes	Yes
DS-X9304-SMIP	4-port 1-, 2-Gbps IP Switching Module	Yes	Yes	Yes	Yes	Yes

1. In software releases earlier than Cisco NX-OS Release 3.3(5a), the Supervisor-2A module appears as unsupported hardware in Device Manager, but the Supervisor-2A module does work with Cisco NX-OS release 3.x software.
2. Cisco SAN-OS Release 3.2(1) and later support the 18/4-Port Multiservice Module (MSM-18/4).

Software Download Process

Use the software download procedure to upgrade to a later version, or downgrade to an earlier version, of an operating system. This section describes the software download process for the Cisco MDS NX-OS software and includes the following topics:

- Determining the Software Version, page 13
- Determining Software Version Compatibility, page 13
- Downloading Software, page 14
- Selecting the Correct Software Image for an MDS 9100 Series Switch, page 15
- Selecting the Correct Software Image for an MDS 9200 Series Switch, page 15
- Selecting the Correct Software Image for an MDS 9500 Series Switch, page 15
- NPE Software Images, page 16

Determining the Software Version

To determine the version of Cisco MDS NX-OS or SAN-OS software currently running on a Cisco MDS 9000 Family switch using the CLI, log in to the switch and enter the **show version** EXEC command.

To determine the version of Cisco MDS NX-OS or SAN-OS software currently running on a Cisco MDS 9000 Family switch using Cisco DCNM for SAN, view the Switches tab in the Information pane, locate the switch using the IP address, logical name, or WWN, and check its version in the Release column.

Determining Software Version Compatibility

Table 7 lists the software versions that are compatible in a mixed SAN environment, the minimum software versions that are supported, and the versions that have been tested. We recommend that you use the latest software release supported by your vendor for all Cisco MDS 9000 Family products.

Table 7 Software Release Compatibility

Cisco NX-OS Software	Minimum NX-OS or SAN-OS Release	Tested NX-OS and SAN-OS Releases
NX-OS Release 5.2(6)	NX-OS Release 5.0(1a) or later	NX-OS Release 5.0(1a) and later
	NX-OS Release 4.2(3) or later	NX-OS Release 4.2(3) and later
	SAN-OS Release 3.3(5) or later	SAN-OS Release 3.3(5) and later

Downloading Software

The Cisco MDS NX-OS software is designed for mission-critical high availability environments. To realize the benefits of nondisruptive upgrades on the Cisco MDS 9500 Directors, we highly recommend that you install dual supervisor modules.

To download the latest Cisco MDS NX-OS software, access the Software Center at this URL:

http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm

See the following sections in this release note for details on how you can nondisruptively upgrade your Cisco MDS 9000 switch. Issuing the **install all** command from the CLI, or using Cisco DCNM for SAN to perform the downgrade, enables the compatibility check. The check indicates if the upgrade can happen nondisruptively or disruptively depending on the current configuration of your switch and the reason.

```
Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes  non-disruptive       rolling
     2       yes      disruptive       rolling  Hitless upgrade is not supported
     3       yes      disruptive       rolling  Hitless upgrade is not supported
     4       yes  non-disruptive       rolling
     5       yes  non-disruptive         reset
     6       yes  non-disruptive         reset
```

At a minimum, you need to disable the default device alias distribution feature using the **no device-alias distribute** command in global configuration mode. The **show incompatibility system bootflash:***system image filename* command determines which additional features need to be disabled.

Note If you would like to request a copy of the source code under the terms of either GPL or LGPL, please send an e-mail to mds-software-disclosure@cisco.com.

Selecting the Correct Software Image for an MDS 9100 Series Switch

The system and kickstart image that you use for an MDS 9100 series switch depends on which switch you use, as shown in Table 8.

Table 8 Software Images for MDS 9100 Series Switches

Cisco MDS 9100 Series Switch Type	Naming Convention
MDS 9134, MDS 9124, Cisco MDs 4-Gbps Fabric Switch for HP c-Class BladeSystem, Cisco MDS 4-Gbps Fabric Switch for IBM BladeCenter	Filename begins with m9100-s2ek9
MDS 9148, Cisco MDS 8Gb Fabric Switch for HP c-Class BladeSystem	Filename begins with m9100-s3ek9

Selecting the Correct Software Image for an MDS 9200 Series Switch

The system and kickstart image that you use for an MDS 9200 series switch depends on which switch you use, as shown in Table 9.

Table 9 Software Images for MDS 9200 Series Switches

Cisco MDS 9200 Series Switch Type	Naming Convention
MDS 9222i	Filename begins with m9200-s2ek9

Selecting the Correct Software Image for an MDS 9500 Series Switch

The system and kickstart image that you use for an MDS 9500 Series are for switches with a Supervisor-2 module, as shown in Table 10. Cisco NX-OS Release 5.x and Release 4.x do not support the Supervisor-1 module.

Table 10 Software Images for Supervisor Type

Cisco MDS 9500 Series Switch Type	Supervisor Module Type	Naming Convention
MDS 9513, 9509, and 9506	Supervisor-2 module Supervisor-2A module	Filename begins with m9500-sf2ek9

Use the **show module** command to display the type of supervisor module in the switch. The following is sample output from the **show module** command on a Supervisor 2 module:

```
switch# show module
Mod  Ports  Module-Type                       Model              Status
---  -----  --------------------------------- ------------------ ------------
...
...
7    0      Supervisor/Fabric-2               DS-X9530-SF2-K9    active *
8    0      Supervisor/Fabric-2               DS-X9530-SF2-K9    ha-standby
```

NPE Software Images

No payload encryption (NPE) images are available with some releases of Cisco MDS NX-OS Release 5.2(x) software. The NPE images are intended for countries who have import restrictions on products that encrypt payload data.

To differentiate an NPE image from the standard software image, the letters npe are included in the image name as follows:

- m9500-sf2ek9-kickstart-mz-npe.5.2.2.bin
- m9500-sf2ek9-mz-npe.5.2.2.bin

When downloading software, ensure that you select the correct software images for you Cisco MDS 9000 Series switch. Nondisruptive software upgrades or downgrades between NPE images and non-NPE images are not supported.

Upgrading Your Cisco MDS NX-OS Software Image

This section lists the guidelines recommended for upgrading your Cisco MDS NX-OS software image and includes the following topics:

- Upgrading Guidelines Specific to NX-OS Release 5.2(6), page 16
- General Upgrading Guidelines, page 18
- Nondisruptive Upgrade Paths, page 18
- FICON Supported Releases and Upgrade Paths, page 19

Note Before you begin the upgrade process, review the list of chassis and modules that Cisco MDS NX-OS Release 5.2(6) supports. See the "MDS 9000 Chassis and Module Support" section on page 9.

For detailed instructions for performing a software upgrade using Cisco DCNM, see the *Cisco DCNM Release Notes, Release 5.2*, which is available from the following website:

http://www.cisco.com/en/US/products/ps10495/prod_release_notes_list.html

Upgrading Guidelines Specific to NX-OS Release 5.2(6)

Follow these guidelines when upgrading to Cisco MDS NX-OS Release 5.2(6):

- Follow the upgrade path to NX-OS Release 5.2(6) that is specified in Table 11.
- An upgrade from Cisco NX-OS Release 4.2(7dE5) to Release 5.2(6) will fail if more than 511 IOA tape acceleration flows are configured.
- Upgrade to NX-OS Release 5.2(x) before you install any Generation 4 module in an MDS 9500 Series switch. Generation 4 modules include the FCoE module and the 32-port and 48-port 8-Gbps Advanced Fibre Channel modules. NX-OS Release 5.2(x) is needed for the switch to recognize the new hardware.
- Perform a full switch reload on an MDS 9509 or MDS 9506 switch after you install NX-OS Release 5.2(1) and install any Generation 4 module, including the FCoE module. The switch reload is required for the new hardware to come up. Once you perform the switch reload, the fabric mode changes to support the Generation 4 hardware. Because of the changed fabric mode, you cannot

subsequently perform a nondisruptive software downgrade from NX-OS Release 5.2(1). For additional information, see the "Downgrading Guidelines Specific to NX-OS Release 5.2(6)" section on page 21.

- Ensure that you have a Supervisor-2A module (DS-X9530-SF2A-K9) installed in a MDS 9500 Series switch if you plan to use the Cisco MDS 9000 8-port 10-Gbps Fibre Channel over Ethernet (FCoE) (DS-X9708-K9).
- We recommend that you delete any SPAN configuration, Fibre Channel tunnel, or tunnel-ID map configuration from your switch before you start the upgrade to NX-OS Release 5.2(1). You can save the SPAN destination and SPAN target configuration and then reconfigure the SPAN session following the upgrade. All SPAN destination and SPAN target ports are reinitialized after the upgrade. To gather information about SPAN sessions and delete them, use the following commands in this order:
  - **show incompatibility systems bootflash:***image_name* to display any incompatible configurations
  - **show span session** to check the current configuration for a SPAN session
  - **no span session** *session-number* to delete a SPAN session
  - **show running-config | include fc-tunnel** to check the current Fibre Channel tunnel configuration
  - **no interface fc-tunnel** *y* to delete a Fibre Channel tunnel on the switch that is the source for the Fibre Channel tunnel
  - **show interface brief | include SD** to check the current configuration for a SPAN destination port configuration
  - **show interface brief | include ST** to check the current configuration for a SPAN target port configuration
  - **no fc-tunnel tunnel-map** *z* **interface** *x/y* to remove an Fibre Channel tunnel map
  - **no switchport mode sd** to negate the SPAN destination port mode for the SPAN destination port
  - **no switchport mode st** to negate the SPAN target port mode for the SPAN target port
- If you are using IVR non-NAT mode, migrate to IVR-NAT mode before you upgrade to NX-OS Release 5.2(1). IVR non-NAT mode is deprecated in NX-OS Release 5.2(1).

Note In dual SAN fabrics, IVR traffic can use one fabric while the other fabric is migrating. Only IVR traffic is disrupted during the migration. Regular traffic within the VSAN is not disrupted during the migration.

To migrate to IVR-NAT mode, follow these steps:

1. Stop or divert all applications on servers that depend on IVR.
   - If CFS distribution is not enabled for IVR, then perform steps 2 through 4 on all switches where IVR is enabled.
   - If CFS distribution is enabled for IVR, then enter the **ivr commit** command following step 2, step 3, and step 4 to distribute the changes to other switches.
2. Deactivate the IVR zone set by entering the **no ivr zoneset activate** command.
3. Enable IVR NAT by entering the **ivr nat** command.
4. Activate the IVR zone set by entering the **ivr zoneset activate** command.
5. Start or re-establish all application that were stopped in step 1.

The network can now run in IVR-NAT mode.

General Upgrading Guidelines

Follow these general guidelines before performing a software upgrade:

- Review the nondisruptive upgrade path to release 5.2(6) in Table 11.
- Install and configure dual supervisor modules before the upgrade.
- Issue the **show install all impact** *upgrade-image* CLI command to determine if your upgrade will be nondisruptive.
- Be aware that some features impact whether an upgrade is disruptive or nondisruptive:
  - **Fibre Channel Ports**: Fibre Channel ports can be nondisruptively upgraded without affecting traffic on the ports. See Table 11 for the nondisruptive upgrade path for all NX-OS and SAN-OS releases.
  - **Gigabit Ethernet Ports**: Traffic on Gigabit Ethernet ports is disrupted during an upgrade or downgrade. This includes IPS modules and the Gigabit Ethernet ports on the MSM-18/4 module and the MDS 9222i switch. Those nodes that are members of VSANs traversing an FCIP ISL are impacted, and a fabric reconfiguration occurs. iSCSI initiators connected to the Gigabit Ethernet ports lose connectivity to iSCSI targets while the upgrade is in progress.
  - **FICON**: If you have FICON enabled, the upgrade path is different. See the "FICON Supported Releases and Upgrade Paths" section on page 19.

Note In addition to these guidelines, you may want to review the information in the "Limitations and Restrictions" section prior to a software upgrade to determine if a feature may possibly behave differently following the upgrade.

Nondisruptive Upgrade Paths

Use Table 11 to determine your nondisruptive upgrade path to Cisco MDS NX-OS Release 5.2(6). Find the image release number you are currently using in the "Current Release" column of the table and follow the steps in the order specified to perform the upgrade.

Note The software upgrade information in Table 11 applies only to Fibre Channel switching traffic. Upgrading system software disrupts IP traffic and intelligent services traffic.

Note Before upgrading to Cisco MDS NX-OS Release 5.2(6) on a Cisco MDS 9509 or 9506 switch, see Table 14 for specific guidelines.

Caution Upgrading to Cisco NX-OS Release 5.2(6) without first upgrading to Release 5.0(x) is not recommended and is not supported, and might result in configuration loss. If you are upgrading to Cisco NX-OS Release 5.2(6) from any release other than Release 5.2(2d), Release 5.2(2a), Release 5.2(2), or Release 5.2(1) the only supported upgrade path to Release 5.2(6) is from Release 5.0(x).

Table 11 Nondisruptive Upgrade Path to Cisco MDS NX-OS Release 5.2(6)

Current Release	Nondisruptive Upgrade Path and Ordered Upgrade Steps
NX-OS:	
Release 5.2(1) and 5.2(2), 5.2(2a), and 5.2(2d)	Upgrade directly to NX-OS Release 5.2(6).
All 5.0(x) releases	Upgrade directly to NX-OS Release 5.2(6).
All 4.2(x) releases and 4.1(x) releases	1. Upgrade to NX-OS Release 5.0(x). 2. Upgrade to NX-OS Release 5.2(6).
SAN-OS:	
Release 3.3(2), 3.3(3), 3.3(4x), and 3.3(5x).	1. Upgrade to NX-OS Release 4.2(9). 2. Upgrade to NX-OS Release 5.0(x). 3. Upgrade to NX-OS Release 5.2(6).
Release 3.3(1c), all 3.2(x), 3.1(x), and 3.0(x) releases)	1. Upgrade to SAN-OS Release 3.3(5b). 2. Upgrade to NX-OS Release 4.2(9). 3. Upgrade to NX-OS Release 5.0(x). 4. Upgrade to NX-OS Release 5.2(6).
Release 2.1(3), 2.1(2e), 2.1(2d), and 2.1(2b)	1. Upgrade to SAN-OS Release 3.3(1c). 2. Upgrade to SAN-OS Release 3.3(5b) 3. Upgrade to NX-OS Release 4.2(9). 4. Upgrade to NX-OS Release 5.0(x). 5. Upgrade to NX-OS Release 5.2(6).
Release 2.1(2), 2.1(1b), 2.1(1a), and 2.0(x)	1. Upgrade to SAN-OS Release 2.1(2b), 2.1(2d), 2.1(2e), or 2.1(3) 2. Upgrade to SAN-OS Release 3.3(1c). 3. Upgrade to SAN-OS Release 3.3(5b) 4. Upgrade to NX-OS Release 4.2(9). 5. Upgrade to NX-OS Release 5.0(x). 1. Upgrade to NX-OS Release 5.2(6)
Release 1.x	1. Upgrade to SAN-OS Release 1.3(4a). 2. Upgrade to SAN-OS Release 2.1(2b). 3. Upgrade to SAN-OS Release 3.3(1c). 4. Upgrade to SAN-OS Release 3.3(5b). 5. Upgrade to NX-OS Release 4.1(x) or 4.2(x). 6. Upgrade to NX-OS Release 5.0(x). 7. Upgrade to NX-OS Release 5.2(6).

FICON Supported Releases and Upgrade Paths

Cisco MDS NX-OS Release 5.2(6) is not a FICON-certified release.

Table 12 lists the SAN-OS and NX-OS releases that are certified for FICON. Refer to the specific release notes for FICON upgrade path information.

Table 12 FICON Supported Releases

FICON Supported Releases	
NX-OS	Release 5.2(2)
	Release 4.2(7b)
	Release 4.2(1b)
	Release 4.1(1c)
SAN-OS	Release 3.3(1c)
	Release 3.2(2c)
	Release 3.0(3b)
	Release 3.0(3)
	Release 3.0(2)
	Release 2.0(2b)

Use Table 13 to determine the nondisruptive upgrade path for FICON-certified releases. Find the image release number you are currently using in the Current Release with FICON Enabled column of the table and follow the recommended path.

Table 13 FICON Nondisruptive Upgrade Path

Current Release with FICON Enabled	Upgrade Path
NX-OS Release 4.2(7b)	You can nondisruptively upgrade directly to NX-OS Release 5.2(2).
NX-OS Release 4.2(1b)	You can nondisruptively upgrade directly to NX-OS Release 4.2(7b).
NX-OS Release 4.1(1c)	You can nondisruptively upgrade directly to NX-OS Release 4.2(1b).
SAN-OS Release 3.3(1c)	You can nondisruptively upgrade directly to NX-OS Release 4.2(1b).
SAN-OS Release 3.2(2c), 3.0(3b), 3.0(3), and 3.0(2).	First upgrade to SAN-OS Release 3.3(1c), and then upgrade to NX-OS Release 4.2(1b).

Downgrading Your Cisco MDS SAN-OS Software Image

This section lists the guidelines recommended for downgrading your Cisco MDS SAN-OS software image and includes the following topics:

- Downgrading Guidelines Specific to NX-OS Release 5.2(6), page 21
- General Downgrading Guidelines, page 22
- NX-OS Release 5.2(x) and Release 5.0(x) Software Downgrade and Upgrade Matrix for Cisco MDS 9509 and 9506 Switches, page 23

Downgrading Guidelines Specific to NX-OS Release 5.2(6)

The following guidelines applies to a downgrade from Cisco MDS NX-OS Release 5.2(6):

- Cisco NX-OS Release 5.2(6) supports IDLE as a fill word for the **switchport fill-pattern** command. Releases earlier than Release 5.2(6) supported only the ARBFF fill word. As a result, when you downgrade from Cisco NX-OS Release 5.2(6) to an earlier release that does not support the IDLE fill word, the following syntax error occurs:

  ```
  Syntax error while parsing 'switchport fill-pattern IDLE speed 8000'
  ```

  The syntax error message is harmless and can be ignored.

- You cannot nondisruptively downgrade from NX-OS Release 5.2(6) to NX-OS Release 5.0(x) if you installed NX-OS Release 5.2(6) on an MDS 9509 or MDS 9506 switch and you installed a Generation 4 module in the switch and performed a full switch reload. The reason for this restriction is the change in fabric mode that occurs following the switch reload with the Generation 4 hardware installed. The downgrade will be disruptive, even if you remove the Generation 4 module prior to starting the downgrade.

  If you do not install Generation 4 hardware or perform a full switch reload following the installation of NX-OS Release 5.2(6) on an MDS 9509 or MDS 9506 switch, then you can nondisruptively downgrade to NX-OS Release 5.0(x).

- If you have the Storage Media Encryption (SME) application configured on your system, you must delete signature clusters when downgrading from Cisco NX-OS Release 5.2(6) to Release 5.2(1).

- Following a ISSD from Cisco NX-OS Release 5.2(6) to an earlier Release 5.2(x) or to Release 5.0(x) on a Cisco MDS 9000 switch that is configured with IVR or FCR, reload the modules with the ELS trap entry. In the case of FCR, reload the module with the FCR device logged in. For IVR, all modules should be reloaded.

- We recommend that you delete any SPAN configuration, Fibre Channel tunnel, or tunnel-ID map configuration from your switch before you downgrade from NX-OS Release 5.2(6) to a lower version. If any SPAN session, SPAN destination, SPAN target, or Fibre Channel tunnel interface is configured, the installer should detect it and prompt you to delete these configurations.

  To gather information about SPAN sessions and delete them, use the following commands in this order:

  - **show incompatibility systems bootflash:***image_name* to display any incompatible configurations
  - **show span session** to check the current configuration for a SPAN session
  - **no span session** *session-number* to delete a SPAN session
  - **show running-config | include fc-tunnel** to check the current Fibre Channel tunnel configuration
  - **no interface fc-tunnel** *y* to delete a Fibre Channel tunnel on the switch that is the source for the Fibre Channel tunnel
  - **show interface brief | include SD** to check the current configuration for a SPAN destination port configuration
  - **show interface brief | include ST** to check the current configuration for a SPAN target port configuration
  - **no fc-tunnel tunnel-map** *z* **interface** *x/y* to remove an Fibre Channel tunnel map
  - **no switchport mode sd** to negate the SPAN destination port mode for the SPAN destination port

  - **no switchport mode st** to negate the SPAN target port mode for the SPAN target port

General Downgrading Guidelines

Follow these general guidelines before you perform a a software downgrade:

- Issue the system **no acl-adjacency-sharing** execute command to disable ACL adjacency usage on Generation 2 and Generation 1 modules. If this command fails, reduce the number of zones, IVR zones, TE ports, or a combination of these in the system and issue the command again.
- Disable all features not supported by the downgrade release. Use the **show incompatibility system** *downgrade-image* command to determine what you need to disable.
- Use the **show install all impact** *downgrade-image* command to determine if your downgrade will be nondisruptive.
- Be aware that some features impact whether a downgrade is disruptive or nondisruptive:
  - **FCoE:** Fibre Channel over Ethernet requires Cisco NX-OS Release 5.2(x). A downgrade from Release 5.2(x) disrupts and stops all FCoE traffic.
  - **Fibre Channel Ports**: Fibre Channel ports can be nondisruptively downgraded without affecting traffic on the ports. See Table 15 for the nondisruptive downgrade path for all SAN-OS releases.
  - **Gigabit Ethernet Ports**: Traffic on Gigabit Ethernet ports is disrupted during a downgrade. This includes IPS modules and the Gigabit Ethernet ports on the MSM-18/4 module, and the MDS 9222i switch. Those nodes that are members of VSANs traversing an FCIP ISL are impacted, and a fabric reconfiguration occurs. iSCSI initiators connected to the Gigabit Ethernet ports lose connectivity to iSCSI targets while the downgrade is in progress.
  - **FICON**: If you have FICON enabled, the downgrade path is different. See the "FICON Downgrade Paths" section on page 25.

NX-OS Release 5.2(x) and Release 5.0(x) Software Downgrade and Upgrade Matrix for Cisco MDS 9509 and 9506 Switches

See the compatibility information in Table 14 to determine if a downgrade to, or upgrade from Release 5.0(x) software is disruptive or nondisruptive on a Cisco MDS 9509 or 9506 switch.

Table 14 NX-OS Release 5.2(x) and Release 5.0(x) Downgrade and Upgrade Matrix

Downgrade Path on a Cisco MDS 9509 or 9506 Switch			
Current Release	**Desired Release**	**Expected Behavior**	**Observed Behavior**
5.2(6)	5.2(2d), 5.2(2a), or 5.2(1)	Nondisruptive	Nondisruptive
5.2(2d)	5.2(2a) or 5.2(1)	Nondisruptive	Nondisruptive
5.2(x)	5.0(7) or 5.0(8)	Disruptive	Disruptive
5.0(7) or 5.0(8)	5.0(1a), 5.0(1b), or 5.0(4)	Disruptive	Nondisruptive The user is expected to explicitly reload the switch using the **reload** command.
5.0(7) or 5.0(8)	4.2(x) or 4.1(x)	Disruptive	Disruptive
5.0(4)	5.0(1a)	Nondisruptive	Nondisruptive
5.0(1a), 5.0(1b), or 5.0(4)	4.2(x) or 4.1(x)	Nondisruptive	Nondisruptive

Upgrade Path on a Cisco MDS 9509 or 9506 Switch			
Current Release	**Desired Release**	**Expected Behavior**	**Observed Behavior**
5.2(1), 5.2(2a), or 5.2(2d)	5.2(6)	Nondisruptive	Nondisruptive
5.2(1) or 5.2(2a)	5.2(2d)	Nondisruptive	Nondisruptive
5.0(7) or 5.0(8)	5.2(x)	Nondisruptive Support for Generation 4 modules is available.	Nondisruptive Support for Generation 4 modules is available.
5.0(1a), 5.0(1b), or 5.0(4)	5.2(x)	Nondisruptive Support for Generation 4 modules is not available.	Nondisruptive Support for Generation 4 modules is not available.

Use Table 15 to determine the nondisruptive downgrade path from Cisco NX-OS Release 5.2(6). Find the NX-OS or SAN-OS image that you want to downgrade to in the To SAN-OS Release column of the table and follow the steps in the order specified to perform the downgrade.

Note The software downgrade information in Table 15 applies only to Fibre Channel switching traffic. Downgrading system software disrupts IP and intelligent services traffic.

Table 15 Nondisruptive Downgrade Path from NX-OS Release 5.2(6)

To NX-OS or SAN-OS Release	Nondisruptive Downgrade Path and Ordered Downgrade Steps
NX-OS:	
Release 5.2(1), 5.2(2), 5.2(2a), and 5.2(2d)	Downgrade directly from NX-OS Release 5.2(6).
All 5.0(x) releases	Downgrade directly from NX-OS Release 5.2(6)[1, 2, 3]
All 4.2(x) and 4.1(x) releases	1. Downgrade to NX-OS Release 5.0(x). 2. Downgrade to NX-OS Release 4.2(x) or 4.1(x).
SAN-OS:	
All 3.3(x) releases	1. Downgrade to NX-OS Release 5.0(x). 2. Downgrade to NX-OS Release 4.2(x) or Release 4.1(x). 3. Downgrade to SAN-OS Release 3.3(x).
All 3.2(x), 3.1(x), 3.0(x) releases, and all 2.1(x) releases.	1. Downgrade to NX-OS Release 5.0(x). 2. Downgrade to NX-OS Release 4.2(x) or Release 4.1(x). 3. Downgrade to SAN-OS Release 3.3(x). 4. Downgrade to SAN-OS Release 3.2(x), Release 3.1(x)., Release 3.0(x), or Release 2.1(x).
All 2.0(x) releases.	1. Downgrade to NX-OS Release 5.0(x). 2. Downgrade to NX-OS Release 4.2(x) or Release 4.1(x). 3. Downgrade to SAN-OS Release 3.3(x). 4. Downgrade to SAN-OS Release 2.1(2x). 5. Downgrade to SAN-OS Release 2.0(x).
Release 1.x	1. Downgrade to NX-OS Release 5.0(x). 2. Downgrade to NX-OS Release 4.2(x) or Release 4.1(x). 3. Downgrade to SAN-OS Release 3.3(x). 4. Downgrade to SAN-OS Release 2.1(2b). 5. Downgrade to SAN-OS Release 1.3(4a). 6. Downgrade to SAN-OS Release 1.x.

1. Before downgrading to NX-OS Release 5.0(8) or Release 5.0(7) on an MDS 9509 or MDS 9506 switch, see "NX-OS Release 5.2(x) and Release 5.0(x) Software Downgrade and Upgrade Matrix for Cisco MDS 9509 and 9506 Switches" section on page 23.
2. If you install a Generation 4 module in an MDS 9509 or MDS 9506 switch and perform a full switch reload following the installation of NX-OS Release 5.2(6), then you cannot nondisruptively download from NX-OS Release 5.2(6) to NX-OS 5.0(x).
3. A downgrade from NX-OS Release 5.2(6) to a release other than Release 5.2(1), 5.2(2), 5.2(2a), or 5.2(2d) disrupts and stops all FCoE traffic because FCoE requires Cisco NX-OS Release 5.2(x).

FICON Downgrade Paths

Table 16 lists the downgrade paths for FICON releases. Find the image release number that you want to downgrade to in the To Release with FICON Enabled column of the table and follow the recommended downgrade path.

Table 16 FICON Downgrade Path

To Release with FICON Enabled	Downgrade Path
NX-OS Release 4.2(7b)	You can nondisruptively downgrade directly from NX-OS Release 5.2(2)
NX-OS Release 4.2(1b)	You can nondisruptively downgrade directly from NX-OS Release 4.2(7b).
NX-OS Release 4.1(1c)	You can nondisruptively downgrade directly from NX-OS Release 4.2(1b).
SAN-OS 3.3(1c)	You can nondisruptively downgrade directly from NX-OS Release 4.1(1c).
SAN-OS 3.2(2c)	First downgrade to SAN-OS Release 3.3(1c) and then downgrade to Release 3.2(2c).
SAN-OS 3.0(3b)	First downgrade to SAN-OS Release 3.3(1c) and then downgrade to Release 3.0(3b).
SAN-OS 3.0(2)	First downgrade to SAN-OS Release 3.3(1c) and then downgrade to Release 3.0(2).

New Features in Cisco MDS NX-OS Release 5.2

This section lists the new software and hardware features in Cisco MDS NX-OS Release 5.2. It includes the following topics:

- New Features in Cisco MDS NX-OS Release 5.2(6), page 25
- New Features in Cisco MDS NX-OS Release 5.2(2d), page 26
- New Features in Cisco MDS NX-OS Release 5.2(2d), page 26
- New Features in Cisco MDS NX-OS Release 5.2(2), page 27
- New Features in Cisco MDS NX-OS Release 5.2(1), page 28
- New Hardware in Cisco MDS NX-OS Release 5.2(1), page 29

Product information about Cisco MDS 9000 NX-OS software is available at this link:

http://www.cisco.com/en/US/products/ps5989/index.html

New Features in Cisco MDS NX-OS Release 5.2(6)

Cisco MDS NX-OS Release 5.2(6) includes the new features described in the following sections:

- Smart Zoning, page 26
- Storage Media Encryption Features, page 26

Smart Zoning

Cisco smart zoning simplifies zoning to reduce the burden on administrators and enable automation of SAN provisioning without affecting SAN hardware resource consumption. When the smart zoning feature is enabled, Cisco MDS 9000 Family fabrics provision the hardware access control entries specified by the zone set more efficiently. Administrators can define zones as one-to-many, or many-to-many without incurring a penalty in switch resource consumption. As a result, zones can be defined to correspond to entities that are meaningful in their data center operations. For example, they can define a zone for an application, or for an application cluster, or for a hypervisor cluster without compromising internal resource utilization.

Follow these guidelines for smart zoning:

- Smart zoning requires that all Cisco MDS 9000 Family switches in the fabric use Cisco MDS 9000 NX-OS Software Release 5.2(6) or later and have the smart zoning feature enabled.
- Smart zoning cannot be enabled if the fabric contains third-party switches or switches running earlier versions of Cisco MDS 9000 NX-OS or SAN-OS software.
- Once you enable smart zoning, you cannot add a switch to the fabric that does not support smart zoning.
- Before downgrading from a switch that has smart zoning enabled, disable smart zoning on all VSANs; otherwise, the downgrade is disruptive.

Note Smart zoning is not supported in a fabric if DMM, IOA, or SME is running. Do not enable smart zoning on a switch where DMM, IOA, or SME is configured.

For additional information on how to implement and configure Smart Zoning, see the *Cisco MDS 9000 Fabric Configuration Guide.*

Storage Media Encryption Features

Cisco NX-OS Release 5.2(6) includes the following enhancements to Cisco Storage Media Encryption (SME) Disk:

- SME Disk now supports greater than 2 TB LUNs for both signature and non-signature mode.
- SME Disk signature mode allows snapshots of a crypto LUN across key change operations.
- SME Disk signature mode automatically recognizes snapshots that are exposed to the host, based on the media signature.
- SME Disk now supports Master Key Rekey (MKR) on a cluster for both signature and non-signature mode.

These enhancements require Cisco NX-OS Release 5.2(6) and Cisco DCNM Release 6.1(1a). For more information on these feature enhancements, see the *Cisco MDS 9000 Family NX-OS Storage Media Encryption Configuration Guide.*

New Features in Cisco MDS NX-OS Release 5.2(2d)

Cisco MDS NX-OS Release 5.2(2d) is a maintenance release that includes bug fixes. It does not include any new features.

New Features in Cisco MDS NX-OS Release 5.2(2a)

Cisco MDS NX-OS Release 5.2(2a) is a maintenance release that includes bug fixes and the following feature enhancement:

- Port Monitor

  Port monitoring has been enhanced with several ASIC counters that monitor and report internal packet drops.

  Additional information about this feature enhancement is available in the *Cisco MDS 9000 Series Interfaces Configuration Guide.*

New Features in Cisco MDS NX-OS Release 5.2(2)

Cisco MDS NX-OS Release 5.2(2) is a FICON-certified version of Cisco MDS NX-OS Release 5.2(1), that also includes new features and bug fixes. In addition to these features, Cisco MDS NX-OS Release 5.2(2) supports all the new software features and new hardware that were introduced in Cisco MDS NX-OS Release 5.2(1).

Cisco MDS NX-OS Release 5.2(2) supports the following software features:

- FICON Certification

  Cisco MDS NX-OS Release 5.2(2) is a FICON-certified release that supports these features:

  - Nondisruptive software upgrades to and downgrades from Cisco NX-OS Release 4.2(7b), which is the previous FICON-certified release.
  - FICON FCIP on the Cisco MDS 9000 SSN-16 module, including FICON Tape Acceleration and XRC Acceleration.
  - FICON Tape Acceleration for ESCON through Optica PRIZM.
  - FICON support on the Cisco MDS 9000 32-port 8-Gbps Advanced Fibre Channel Switching module, the Cisco MDS 9000 48-port 8-Gbps Advanced Fibre Channel Switching module, and the Cisco MDS 9513 Switching Fabric 3 module (DS-13SLT-FAB3).

- Availability of Cisco MDS NX-OS Release 5.2 on Cisco MDS 9100 Series Fabric Switches

  Cisco MDS NX-OS Release 5.2(2) supports the following switches (which are not supported by Cisco MDS NX-OS Release 5.2(1)):

  - Cisco MDS 9134 Fabric Switch
  - Cisco MDS 9124 Fabric Switch
  - Cisco MDs 4-Gbps Fabric Switch for HP c-Class BladeSystem
  - Cisco MDS 4-Gbps Fabric Switch for IBM BladeCenter

- Port Group Monitoring

  Port group monitoring and SNMP are available on the Cisco MDS 9000 32-port 8-Gbps Advanced Fibre Channel Switching module and the Cisco MDS 9000 48-port 8-Gbps Advanced Fibre Channel Switching module.

- Availability of IVR on the Cisco MDS 9148 Switch

  Cisco MDS NX-OS Release 5.2(2) supports Inter-VSAN Routing (IVR) on the Cisco MS 9148 multilayer fabric switch.

- IOA with NPV

Cisco MDS NX-OS Release 5.2(2) supports configuring IOA with NPV.

New Features in Cisco MDS NX-OS Release 5.2(1)

Cisco MDS NX-OS Release 5.2(1) supports the following software features:

- Software support for the MDS 9000 8-port 10-Gbps Fibre Channel over Ethernet (FCoE) module

  The MDS 9000 8-port 10-Gbps Fibre Channel over Ethernet (FCoE) module is a multihop-capable FCoE module for the core data center. This full line-rate FCoE module for the MDS 9500 Series Director switches allows you to extend FCoE benefits beyond the access Layer into the data center core. FCoE supports I/O consolidation by preserving all Fibre Channel constructs, and maintaining the same latency, security, and traffic management attributes of Fibre Channel. In addition, FCoE extends Fibre Channel SAN connectivity to Cisco Nexus 7000 switches that are FCoE capable.

- Software support for Cisco MDS 9000 Family 8-Gbps Advanced Fibre Channel Switching Modules

  Cisco NX-OS Release 5.2(1) includes software support for the 32-port and the 48-port 8-Gbps Advanced Fibre Channel switching modules that can be used in the MDS 9500 Series Directors. The MDS 9513 Multilayer Director can be upgraded with the new Generation 4 Fabric-3 module to increase bandwidth to 256 Gbps per slot. In addition, the 8-Gbps Advance Fibre Channel switching module support speeds of 10 Gbps on the MDS 9513 with the Fabric-3 module installed. The upgrade from the Fabric-2 module to the Fabric-3 module is nondisruptive.

  Cisco MDS 9000 8-Gbps Advanced Fibre Channel switching modules support Cisco FlexSpeed technology that enables ports to be configured as either 1-, 2-, 4-, or 8-Gbps, or 10-Gbps Fibre Channel interfaces.

  Cisco MDS 9000 8-Gbps Advanced Fibre Channel switching modules support Arbitrated Local Switching to locally switch traffic at line rate 8-Gbps in a fair manner across all ports on the module through central arbitration.

- Storage Media Encryption for Disk

  The Storage Media Encryption (SME) solution, which currently protects data at rest on heterogeneous tape drives and virtual tape libraries (VTLs), has been enhanced to encrypt data on disk arrays in a SAN environment using secure IEEE-standard Advanced Encryption Standard (AES) algorithms.

  SME Disk requires the Storage Media Encryption Package license.

  See the *Cisco MDS 9000 Family Storage Media Encryption Configuration Guide* for more information on configuring and deploying SME Disk.

- Cisco Data Center Network Manager for SAN

  Cisco Fabric Manager and Cisco Data Center Network Manager have merged into a unified product that can now manage and monitor both SAN and LAN environments. As a part of this merger, Cisco Fabric Manager has been rebranded as Cisco DCNM for SAN.

  As a part of NX-OS Release 5.2(1), Cisco DCNM for SAN introduces server-based licenses that allow you to purchase a pool of Cisco DCNM for SAN licenses instead of a switch-based Fabric Manager Server (FMS) license. The installed base of existing FMS licenses are grandfathered into Cisco DCNM for SAN, which means that you do not have to purchase a new license to use Cisco DCNM for SAN if you have an existing FMS license.

  There are many new features in Cisco DCNM for SAN, including:

  - Summary and host dashboards
  - VMware topology and performance

- Performance forecasting charts
- External SMI-S 1.4 agent
- FCoE provisioning and management

Detailed information about Cisco DCNM features is available in the *Cisco DCNM Release Notes, Release 5.2,* and in the feature configuration guides for Cisco DCNM for SAN.

For additional information about Cisco MDS NX-OS Release 5.2(1), see the *Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Release 5.2(1).*

New Hardware in Cisco MDS NX-OS Release 5.2(1)

Cisco MDS NX-OS Release 5.2(1) supports the following new Generation 4 hardware devices:

- Cisco MDS 9000 8-port 10-Gbps Fibre Channel over Ethernet (FCoE) module (DS-X9708-K9)
- Cisco MDS 9000 32-port 8-Gbps Advanced Fibre Channel Switching module (DS-X9232-256K9)
- Cisco MDS 9000 48-port 8-Gbps Advanced Fibre Channel Switching module (DS-X9248-256K9)
- Cisco MDS 9513 Switching Fabric 3 module (DS-13SLT-FAB3)

See the *Cisco MDS 9500 Series Hardware Installation Guide* for descriptions of, and specifications for the new Generation 4 modules. This guide also provides instructions for migrating to the new Fabric 3 module and guidelines for installing the new 8-Gbps Advanced Fibre Channel switching modules.

Licensed Cisco NX-OS Software Packages

Most Cisco MDS 9000 family software features are included in the standard package. However, some features are logically grouped into add-on packages that must be licensed separately, such as the Cisco MDS 9000 Enterprise package, SAN Extension over IP package, Mainframe package, Storage Services Enabler (SSE) package, Storage Media Encryption package, and Data Mobility Manager package. On-demand ports activation licenses are also available for the Cisco MDS Blade Switch Series and 4-Gbps Cisco MDS 9100 Series Multilayer Fabric switches.

Note A license is not required to use the Cisco MDS 9000 8-port 10-Gbps Fibre Channel over Ethernet (FCoE) module (DS-X9708-K9).

Enterprise Package

The standard software package that is bundled at no charge with the Cisco MDS 9000 Family switches includes the base set of features that Cisco believes are required by most customers for building a SAN. The Cisco MDS 9000 family also has a set of advanced features that are recommended for all enterprise SANs. These features are bundled together in the Cisco MDS 9000 Enterprise package. Refer to the Cisco MDS 9000 Enterprise package fact sheet for more information.

SAN Extension over IP Package

The Cisco MDS 9000 SAN Extension over IP package allows the customer to use FCIP to extend SANs over wide distances on IP networks using the Cisco MDS 9000 family IP storage services. Refer to the Cisco MDS 9000 SAN Extension over IP package fact sheet for more information.

Mainframe Package

The Cisco MDS 9000 Mainframe package uses the FICON protocol and allows control unit port management for in-band management from IBM S/390 and z/900 processors. FICON VSAN support is provided to help ensure true hardware-based separation of FICON and open systems. Switch cascading, fabric binding, and intermixing are also included in this package. Refer to the Cisco MDS 9000 Mainframe package fact sheet for more information.

Storage Media Encryption Package

The Cisco MDS 9000 Storage Media Encryption package enables encryption of data at rest on heterogeneous tape devices, virtual tape libraries, and disk arrays as a transparent fabric service. Cisco SME is completely integrated with Cisco MDS 9000 Family switches and the Cisco DCNM for SAN application, enabling highly available encryption services to be deployed without rewiring or reconfiguring SANs, and allowing them to be managed easily without installing additional management software. Refer to the Cisco MDS 9000 Storage Media Encryption package fact sheet for more information. The Storage Media Encryption package is for use only with Cisco MDS 9000 Family switches.

Data Mobility Manager Package

The Cisco MDS 9000 Data Mobility Manager package enables data migration between heterogeneous disk arrays without introducing a virtualization layer or rewiring or reconfiguring SANs. Cisco DMM allows concurrent migration between multiple LUNs of unequal size. Rate-adjusted migration, data verification, dual Fibre Channel fabric support, and management using Cisco DCNM for SAN provide a complete solution that greatly simplifies and eliminates most downtime associated with data migration. Refer to the Cisco MDS 9000 Data Mobility Manager package fact sheet for more information. The Data Mobility Manager package is for use only with Cisco MDS 9000 Family switches.

Storage Services Enabler Package

The Cisco MDS 9000 SSE package allows network-based storage applications and services to run on the Cisco MDS 9000 family SSMs, Cisco MDS 9000 18/4-Port Multiservice Module (MSM-18/4), and Cisco MDS 9222i. Intelligent fabric applications simplify complex IT storage environments and help organizations gain control of capital and operating costs by providing consistent and automated storage management. Refer to the Cisco MDS 9000 SSE package fact sheet for more information.

On-Demand Port Activation License

On-demand ports allow customers to benefit from Cisco NX-OS Software features while initially purchasing only a small number of activated ports on 8-Gbps or 4-Gbps Cisco MDS 9100 Series Multilayer Fabric switches. As needed, customers can expand switch connectivity by licensing additional ports.

I/O Accelerator Package

The Cisco I/O Accelerator (IOA) package activates IOA on the Cisco MDS 9222i fabric switch, the Cisco MDS 9000 18/4 Multiservice Module (MSM-18/4), and on the SSN-16 module. The IOA package is licensed per service engine and is tied to the chassis. The number of licenses required is equal to the number of service engines on which the intelligent fabric application is used.The SSN-16 requires a separate license for each engine on which you want to run IOA. Each SSN-16 engine that you configure for IOA checks out a license from the pool managed at the chassis level. SSN-16 IOA licenses are available as single licenses.

XRC Acceleration License

The Cisco Extended Remote Copy (XRC) acceleration license activates FICON XRC acceleration on the Cisco MDS 9222i switch and on the MSM-18/4 in the Cisco MDS 9500 Series directors. One license per chassis is required. You must install the Mainframe Package and the SAN Extension over FCIP Package before you install the XRC acceleration license. The Mainframe Package enables the underlying FICON support, and the FCIP license or licenses enable the underlying FCIP support.

Deprecated Features

Cisco MDS NX-OS Release 5.2 no longer supports the features listed in the following sections:

- Zoning Features, page 31
- SNIA Common Information Model, page 32
- IVR Non-NAT Mode, page 32

Zoning Features

LUN zoning, read-only zones, and broadcast zones are no longer supported. These features affect the following hardware:

- Cisco MDS 9000 8-port 10-Gbps Fibre Channel over Ethernet (FCoE) module
- Cisco MDS 9000 48-port 8-Gbps Advanced Fibre Channel Switching module
- Cisco MDS 9000 32-port 8-Gbps Advanced Fibre Channel Switching module

You cannot bring up these modules if these features are already configured. You should completely remove all configurations that include these features before you attempt to bring up these modules. In addition, you cannot configure these features after you bring up these modules.

SNIA Common Information Model

SNIA Common Information Model (CIM or cimserver) commands are no longer supported. CIM is supported in Cisco DCNM-SAN Release 5.2. The SMI-S agent that is installed on the Cisco DCNM-SAN server allows external application to access fabric and switch profiles as specified in SNIA CIM. For additional information, see the *Cisco DCNM Release Notes, Release 5.2*.

IVR Non-NAT Mode

IVR non-NAT mode is not supported in Cisco NX-OS Release 5.2(x). If you have IVR non-NAT mode configured, see the "Upgrading Guidelines Specific to NX-OS Release 5.2(6)" section on page 16 for instructions on how to migrate to IVR NAT mode before upgrading to Cisco NX-OS Release 5.2(6).

Limitations and Restrictions

This section lists the limitations and restrictions. The following limitations are described:

- SME Quorum, page 33
- OUI Mismatch for SME Tape Targets, page 33
- FCIP Performance Drop, page 33
- FCoE Module, page 33
- IPv6, page 33
- User Roles, page 33
- Schedule Job Configurations, page 34
- Maximum Number of Zones Supported in Interop Mode 4, page 34
- InterVSAN Routing, page 34
- Java Web Start, page 34
- VRRP Availability, page 34
- Using a RSA Version 1 Key for SSH Following an Upgrade, page 35
- CFS Cannot Distribute All Call Home Information, page 35
- Availability of F Port Trunking and F Port Channels, page 36
- Reserved VSAN Range and Isolated VSAN Range Guidelines, page 36
- Applying Zone Configurations to VSAN 1, page 37
- Running Storage Applications on the MSM-18/4, page 37
- RSPAN Traffic Not Supported on CTS Ports on 8-Gbps Switching Modules, page 37
- I/O Accelerator Feature Limitations, page 37
- Support for FCIP Compression Modes, page 38
- Saving Copies of the Running Kickstart and System Images, page 38
- Configuring Buffer Credits on a Generation 2 or Generation 3 Module, page 38
- Features Not Supported on the Cisco MDS 9148 Switch, page 38
- PPRC Not Supported with FCIP Write Acceleration, page 39

- Configuring a Persistent FCID in an IVR Configuration with Brocade Switches, page 39

SME Quorum

You cannot change the quorum or the SME master node during a master key rekey. If a change occurs during the smart card portion of the operation, the master key rekey operation will fail and must be repeated from the beginning.

OUI Mismatch for SME Tape Targets

If Cisco DCNM does not discover all expected tape targets, check the sme.log to identify an OUI mismatch. Look for a message like the following:

```
2012.04.09 21:15:50  WARN  [SME]   skipped target 50:06:0b:00:00:b8:e4:b0 due to explicit
type mismatch.  Expect: 240 found: 228.  If this is an error update your OUI definitions
```

To correct this issue, manually add the OUI definitions to the server.properties file. The format is as follows:

```
# 0xhhhhhh vendor_name devicetypes h(host)|d(disk)|t(tape)|s(switch)|g(gateway)|m(cisco
mds)
# for example: newOUIs=0x00E069 JNI h|d; 0x000ded Cisco m;\
# 0x006069 Brocade s;
newOUIs=
```

FCIP Performance Drop

FCIP performance can drop in a topology where the round-trip time (RTT) delay is configured at 80 ms, IPSec is enabled, and write acceleration (WA) is not used.

FCoE Module

- In Cisco MDS NX-OS Release 5.2(x), you cannot install a FCoE module in a switch that is running DMM, SME, or IOA.
- Link traps for FCoE devices are sent only when a VFC interface flaps.

IPv6

The management port on Cisco MDS switches supports one user-configured IPv6 address, but does not support auto-configuration of an IPv6 address.

User Roles

In SAN-OS Release 3.3(x) and earlier, when a user belongs to a role which has a VSAN policy set to Deny and the role allows access to a specific set of VSANs (for example, 1 through 10), the user is restricted from performing the **configuration**, **clear**, **execute**, and **debug** commands which had a VSAN parameter outside this specified set. Beginning with NX-OS Release 4.1(1b), these users are still

prevented from performing **configuration**, **clear**, **execute**, and **debug** commands as before, however, they are allowed to perform **show** commands for all VSANs. The ability to execute the **show** command addresses the following:

- In a network environment, users often need to view information in other VSANs even though they do not have permission to modify configurations in those VSANs.
- This behavior makes Cisco MDS 9000 Series switches consistent with other Cisco products, such as Cisco Nexus 7000 Series switches, that exhibit the same behavior for those roles (when they apply to the VLAN policy).

Schedule Job Configurations

As of MDS NX-OS Release 4.1(1b) and later, the scheduler job configurations need to be entered in a single line with a semicolon(;) as the delimiter.

Job configuration files created with SAN-OS Release 3.3(1c) and earlier, are not supported. However, you can edit the job configuration file and add the delimiter to support Cisco NX-OS Release 4.1(3a).

Maximum Number of Zones Supported in Interop Mode 4

In interop mode 4, the maximum number of zones that is supported in an active zone set is 2047, due to limitations in the connected vendor switch.

When IVR is used in interop mode 4, the maximum number of zones supported, including IVR zones, in the active zone set is 2047.

InterVSAN Routing

When using InterVSAN Routing (IVR), it is recommended to enable Cisco Fabric Services (CFS) on all IVR-enabled switches. Failure to do so may cause mismatched active zone sets if an error occurs during zone set activation.

Java Web Start

When using Java Web Start, it is recommended that you do not use an HTML cache or proxy server. You can use the Java Web Start Preferences panel to view or edit the proxy configuration. To do this, launch the Application Manager, either by clicking the desktop icon (Microsoft Windows), or type **./javaws** in the Java Web Start installation directory (Solaris Operating Environment and Linux), and then select **Edit> Preferences**.

If you fail to change these settings, you may encounter installation issues regarding a version mismatch. If this occurs, you should clear your Java cache and retry.

VRRP Availability

The Virtual Router Redundancy Protocol (VRRP) is not available on the Gigabit Ethernet interfaces on the MSM-18/4 module or module 1 of the MDS 9222i switch, even though it is visible on these modules. The feature is not implemented in the current release.

Using a RSA Version 1 Key for SSH Following an Upgrade

For security reasons, NX-OS Release 4.2(1b) does not support RSA version 1 keys. As a result, if you upgrade to NX-OS Release 4.2(1b) from an earlier version that did support RSA version 1 keys, and you had configured an RSA version 1 key for SSH, then you will not be able to log in through SSH following the upgrade.

If you have an RSA version 1 key configured for SSH, before upgrading to NX-OS Release 4.1(3a), follow these steps:

Step 1 Disable SSH.

Step 2 Create RSA version 2 DSA keys.

Step 3 Enable SSH.

Step 4 Delete any RSA version 1 keys on any remote SSH clients and replace the version 1 keys with the new version 2 keys from the switch.

Proceed with the upgrade to NX-OS Release 4.2(1b).

If you upgrade before disabling SSH and creating RSA version 2 keys, follow these steps:

Step 1 Open a Telnet session and log in through the console.

Step 2 Issue the **no feature ssh** command to disable SSH.

Step 3 Issue the **ssh key rsa 1024** command to create RSA version 2 keys.

Step 4 Issue the **feature ssh** command to enable SSH.

CFS Cannot Distribute All Call Home Information

In MDS NX-OS Release 4.2(1b), CFS cannot distribute the following Call Home commands that can be configured with the **destination-profile** command:

- **destination-profile** *profile_name* **transport-method**
- **destination-profile** *profile_name* **http**

The output of the **show running-config callhome** command shows configured Call Home commands:

```
switch# show running-config callhome
> version 4.1(3)
> callhome
>   email-contact abc@cisco.com <mailto:abc@cisco.com>
>   phone-contact +14087994089
>   streetaddress xyxxyx
>   distribute
>   destination-profile testProfile
>   destination-profile testProfile format XML
>   no destination-profile testProfile transport-method email
>   destination-profile testProfile transport-method http
>   destination-profile testProfile http https://xyz.abc.com
>   destination-profile testProfile alert-group all
>   transport email smtp-server 64.104.140.134 port 25 use-vrf management
>   transport email from abc@cisco.com <mailto:abc@cisco.com>
```

```
>    enable
>    commit
```

When you attempt to apply these commands in the ASCII configuration, the following commands fail:

```
>    no destination-profile testProfile transport-method email
>    destination-profile testProfile transport-method http
>    destination-profile testProfile http https://xyz.abc.com
```

To work around this issue, issue these commands after the **commit** command.

Availability of F Port Trunking and F Port Channels

Trunking F ports and trunking F port channels are not supported on the following MDS 9000 components:

- DS-C9134-K9, Cisco MDS 9134 Multilayer Fabric Switch, if NPIV is enabled and the switch is used as the NPV core switch
- DS-C9124-K9, Cisco MDS 9124 Multilayer Fabric Switch, if NPIV is enabled and the switch is used as the NPV core switch

Trunking F ports, trunking F port channels and regular F port channels are not supported on the following MDS 9000 components:

- DS-X9016, Cisco MDS 9000 2-Gbps16-Port Fibre Channel Switching Module
- DS-X9032, Cisco MDS 9000 2-Gbps 32-Port Fibre Channel Switching Module
- DS-X9032-14K9, Cisco MDS 9000 14/2-Port Multiprotocol Services Module (MPS-14/2)

For configuration information, refer to the "Configuring Trunking" section in the *Cisco MDS 9000 NX-OS Interfaces Configuration Guide*.

Reserved VSAN Range and Isolated VSAN Range Guidelines

On an NPV switch with a trunking configuration on any interface, or on a regular switch where the **feature fport_channel_trunk** command has been issued to enable the Trunking F port channels feature, follow these configuration guidelines for reserved VSANs and the isolated VSAN:

- If trunk mode is on for any of the interfaces or NP port channel is up, the reserved VSANs are 3040 to 4078, and they are not available for user configuration.
- The Exchange Virtual Fabric Protocol (EVFP) isolated VSAN is 4079, and it is not available for user configuration.

The following VSAN IDs are assigned in the Fibre Channel Framing and Signaling (FC-FS) interface standard:

VF_ID Value	Value Description
00h	Do not use as a Virtual Fabric Identifier.
001h ... EFFh	Available as a Virtual Fabric Identifier.
F00h ... FEEh	Reserved.
FEFh	Control VF-ID (see Fibre Channel Link Services (FC-LS) and Fibre Channel Switch Fabric Generation 4 (FC-SW-4) standards).

VF_ID Value	Value Description
FF0h ... FFEh	Vendor specific.
FFFh	Do not use as a Virtual Fabric Identifier.
FEFh = 4079	

Applying Zone Configurations to VSAN 1

In the setup script, you can configure system default values for the default-zone to be permit or deny, and you can configure default values for the zone distribution method and for the zone mode.

These default settings are applied when a new VSAN is created. However, the settings will not take effect on VSAN 1, because it exists prior to running the setup script. Therefore, when you need those settings for VSAN 1, you must explicitly issue the following commands:

- **zone default-zone permit** *vsan 1*
- **zoneset distribute full** *vsan 1*
- **zone mode enhanced** *vsan 1*

Running Storage Applications on the MSM-18/4

The Cisco MDS 9000 18/4-Port Multiservice Module (MSM-18/4) does not support multiple, concurrent storage applications. Only one application, such as SME or DMM, can run on the MSM-18/4 at a time.

RSPAN Traffic Not Supported on CTS Ports on 8-Gbps Switching Modules

An inter-switch link (ISL) that is enabled for Cisco TrustSec (CTS) encryption must be brought up in non-CTS mode to support remote SPAN (RSPAN) traffic on the following modules:

- DS-X9248-96K9: Cisco MDS 9000 48-Port 8-Gbps Fibre Channel Switching Module
- DS-X9224-96K9: Cisco MDS 9000 24-Port 8-Gbps Fibre Channel Switching Module
- DS-X9248-48K9: Cisco MDS 9000 4/44-Port Host-Optimized 8-Gbps Fibre Channel Switching Module

If the ISL link is brought up with CTS enabled, random packet drops of both RSPAN traffic and normal traffic will occur on the receiver port switch.

I/O Accelerator Feature Limitations

IOA does not support the following NX-OS features:

- F port trunking
- F port channeling
- IOA cannot be configured on flows in topologies that have devices with NPV and NPIV enabled. For example, IOA is not supported in a topology where a host logs in from a NPV edge switch and IOA is deployed on a NPV core switch for this host.

Support for FCIP Compression Modes

In Cisco NX-OS Release 4.2(1b) and later, FCIP compression mode 1 and compression mode 3 are not supported on the Cisco MSM-18/4 module and on the SSN-16 module.

Saving Copies of the Running Kickstart and System Images

After you upgrade to MDS NX-OS Release 4.2(1b), you are not allowed to delete, rename, move, or overwrite the kickstart and system images that are in the current system bootvar settings on an active or standby MDS Supervisor-2 module on any Cisco MDS 9500 Series switch. This restriction does not apply to the integrated supervisor module on the MDS 9200 and MDS 9100 series switches.

Configuring Buffer Credits on a Generation 2 or Generation 3 Module

When you configure port mode to auto or E on a Generation 2 module, one of the ports will not come up for the following configuration:

- Port Mode: auto or E for all of the ports
- Rate Mode: dedicated
- Buffer Credits: default value

When you configure port mode to auto or E on a Generation 3 module, one or two of the ports will not come up for the following configuration:

- Port Mode: auto or E for the first half of the ports, the second half of the ports, or for all of the ports
- Rate Mode: dedicated
- Buffer Credits: default value

When you configure port mode to auto or E for all ports in the global buffer pool, you need to reconfigure buffer credits on one or more of the ports. The total number of buffer credits configured for all the ports in the global buffer pool should be reduced by 64.

Features Not Supported on the Cisco MDS 9148 Switch

The Cisco MDS 9148 Multilayer Fabric Switch does not support the following NX-OS features:

- Remote Span
- Translative loop support
- FCC - no generation, quench reaction only
- FC-Redirect

In addition, the following features have these limits:

- VSANs - 31 maximum
- SPAN - 1 session maximum

PPRC Not Supported with FCIP Write Acceleration

IBM Peer to Peer Remote Copy (PPRC) is not supported with FCIP Write Acceleration.

Configuring a Persistent FCID in an IVR Configuration with Brocade Switches

The following information is relevant if you have a fabric that consists of Cisco MDS 9000 switches and Brocade switches, and the Cisco MDS switches are running either NX-OS Release 4.x or Release 5.x and Brocade is running FOS higher than 6.x. In an IVR configuration, when IVR NAT is enabled on a Cisco MDS 9000 switch, the device in the native VSAN should be configured with a persistent FCID. Assuming the FCID is 0xAABBCC, AA should be configured with the virtual IVR domain ID of the VSAN that contains the ISLs and BB should be configured in the following range:

- 1 through 64 if the Brocade switch is operating in native interop mode.
- 1 through 30 if the Brocade switch is operating in McData Fabric mode or McData Open Fabric Mode.

This configuration ensures that the devices connected to the Cisco MDS 9000 switch can be seen in the name server database on the Brocade switch.

Caveats

This section lists the open and resolved caveats for this release. Use Table 17 to determine the status of a particular caveat. In the table, “O” indicates an open caveat and “R” indicates a resolved caveat.

Table 17 Open Caveats and Resolved Caveats Reference

DDTS Number	NX-OS Software Release (Open or Resolved)	NX-OS Software Release (Open or Resolved)
	5.2(2d)	5.2(6)
Severity 1		
CSCua70336	—	R
Severity 2		
CSCtn72391	O	O
CSCtq88900	O	O
CSCtr10877	O	O
CSCtr42293	O	R
CSCtr59985	O	R
CSCtw64713	O	O
CSCtx45067	—	R
CSCty01206	O	R
CSCty59570	—	O
CSCty59664	—	R
CSCty61259	—	R

Table 17 Open Caveats and Resolved Caveats Reference (continued)

DDTS Number	NX-OS Software Release (Open or Resolved)	NX-OS Software Release (Open or Resolved)
	5.2(2d)	5.2(6)
CSCty68838	O	O
CSCty82906	—	O
CSCtz53329	O	O
CSCtz59701	O	R
CSCtz73068	O	R
CSCtz73136	O	R
CSCtz82290	O	R
CSCtz83956	O	R
CSCua04249	—	R
CSCua12379	—	O
CSCua15818	O	R
CSCua47533	O	R
CSCua61044	O	R
CSCua61044	—	R
CSCua84273	—	R
CSCub47799	O	O
CSCub51064	—	O
CSCuc35483	—	O
CSCuc84790	—	O
CSCuf31077	—	O
CSCum30306	O	O
Severity 3		
CSCtr20364	—	R
CSCtr41519	O	R
CSCtr50223	O	O
CSCtr55608	O	R
CSCtr83189	—	R
CSCtr92846	—	R
CSCts16956	—	R
CSCts71286	—	R
CSCts89154	O	R
CSCtu07107	—	R
CSCtu13569	O	R
CSCtw60823	—	R

Table 17 Open Caveats and Resolved Caveats Reference (continued)

DDTS Number	NX-OS Software Release (Open or Resolved)	NX-OS Software Release (Open or Resolved)
	5.2(2d)	5.2(6)
CSCtx02571	O	R
CSCtx17833	—	R
CSCtx35664	—	R
CSCtx41288	—	O
CSCtx77816	—	R
CSCty01555	—	R
CSCty01609	—	R
CSCty13815	O	R
CSCty30802	—	R
CSCty33006	O	R
CSCty57144	O	R
CSCty80115	—	R
CSCty82821	—	O
CSCty97827	O	R
CSCtz04489	—	R
CSCtz13890	—	R
CSCtz15659	—	R
CSCtz23936	O	R
CSCtz25933	O	R
CSCtz44601	O	R
CSCtz56349	—	R
CSCtz69973	—	R
CSCtz85952	O	R
CSCtz99466	—	R
CSCua02159	O	R
CSCua34425	—	R
CSCua37931	O	R
CSCua61011	—	O
CSCua72788	—	R
CSCub09763	—	R
CSCub27133	O	R
CSCub52623	—	O
Severity 4		
CSCtz09820	O	O

Table 17 Open Caveats and Resolved Caveats Reference (continued)

DDTS Number	NX-OS Software Release (Open or Resolved)	NX-OS Software Release (Open or Resolved)
	5.2(2d)	**5.2(6)**
CSCtz19169	O	O
CSCtz40700	O	O
CSCtz40745	O	O
CSCua09712	—	O
Severity 5		
CSCtz84847	—	O
Severity 6		
CSCtr01652	—	R
CSCty47599	—	O
CSCuh27347	O	O

Resolved Caveats

- CSCua70336

  Symptom: The FLOGI process might fail repeatedly, which leads to a system reload if a module reboots during an ISSU or DSSU. This issue can occur only if a module reloads (for any reason) during ISSU or DSSU. This is not a normal event and this issue is not likely to occur.

  Workaround: This issue is resolved.

- CSCtr42293

  Symptom: An IOA tape read acceleration problem occurs when sending Accept (ACC) to the Read Exchange Concise (REC) Extended Link Service with data_xfer_count = 0, and when a few data packets have been sent. Once the REC ACC is sent, the host sends a Sequence Retransmission Request (SRR) FCP FC-4 Link Service Request to claim the rest of the data. The target sends a REJECT, which causes the host to end the exchange. This symptom might be seen when IOA retransmissions occur from target to host.

  Workaround: This issue is resolved.

- CSCtr59985

  Symptom: A tape target is unresponsive and a permanent error is sent to the host. The host side and target side IOA traces show multiple Read Exchange Concise and Sequence Retransmission Request events followed by ABTS for the read exchanges.

  Workaround: This issue is resolved.

- CSCtx45067

  Symptom: A process fails in /isan/bin/xbm when the CPU is mostly occupied by two or three processes and snmpd is one of them.

  This symptom occurs on Cisco MDS 9000 switches running Cisco NX-OS Release 5.0(4d). When there is frequent interaction between snmpd and other processes such as zone, the priority of these processes is promoted. As the result, these two processes and a few others occupy most of the CPU, and other processes do not get to run which causes them to fail, typically due to a heartbeat failure.

Workaround: This issue is resolved.

- CSCty01206

  Symptom: After upgrading Fabric Manager Server and the Cisco Key Management Centers (KMC) from Cisco NX-OS Release 4.2(3) to Release 5.0(4d) to Release 5.2(1), the old tape key replication relationships are lost. However, you are able to create new tape key replication relationships for the newly created tape-backup groups.

  This symptom occurs following an upgrade of the KMC to Cisco NX-OS Release 5.2(1).

  Workaround: This issue is resolved.

- CSCty59664

  Symptom: After releasing the local zone lock through Cisco Fabric Manager, the fabric lock still exists and the IVR commit does not happen.

  Workaround: This issue is resolved.

- CSCty61259

  Symptom: During an ISSU from Cisco NX-OS Release 4.2(3) to Release 5.0(7), the standby supervisor failed to boot to the new version, but the boot variables were modified to the new release, which is not the expected behavior.

  Workaround: This issue is resolved.

- CSCtz53329

  Symptom: The standby supervisor resets and this message is logged in the syslog:

```
  %SYSMGR-2-GSYNC_SNAPSHOT_SRVFAILED: Service "syslogd" on active supervisor
failed to store its snapshot (error-id 0x80480018).
  %SYSMGR-2-STANDBY_BOOT_FAILED: Standby supervisor failed to boot up
```

  Condition: This situation only occurs if the standby supervisor reloads many times.

  Workaround: None.

  More Information: Contact Cisco TAC to recover from this issue.

- CSCtz59701

  Symptom: An EPLD upgrade failed because an incorrect fabric controller was detected.

  Workaround: This issue is resolved.

- CSCtz73068

  Symptom: The ethport process failed on the active supervisor and then on the standby supervisor after a switchover that was triggered by hap-reset, which caused a switch reload.

```
switch# show system reset-reason
----- reset reason for Supervisor-module 5 (from Supervisor in slot 5) ---
1) At 645162 usecs after Wed May  2 11:56:56 2012
    Reason: Reset triggered due to HA policy of Reset
    Service: ethport hap reset
    Version: 5.2(2a)
----- reset reason for Supervisor-module 6 (from Supervisor in slot 6) ---
1) At 685033 usecs after Wed May  2 12:01:03 2012
    Reason: Reset triggered due to HA policy of Reset
    Service: ethport hap reset
    Version: 5.2(2a)
```

  Four core files were created, two for each supervisor module.

```
switch# show cores
Module  Instance  Process-name     PID       Date(Year-Month-Day Time)
```

```
------  --------  ---------------  --------  -------------------------
5       1         ethport          3445      2012-05-02 12:02:36
5       1         ethport          11344     2012-05-02 12:02:38
6       1         ethport          30298     2012-05-02 12:06:47
6       1         ethport          3491      2012-05-02 12:06:49
```

This symptom might occur when a PortChannel is created over Gigabit Ethernet ports.

```
user=admin:cmd=configure terminal ; interface port-channel 1 ; channel mode active
(SUCCESS)
user=admin:cmd=configure terminal ; interface port-channel 1 ; shutdown (SUCCESS)
user=admin:cmd=Interface port-channel 1 state updated to up
user=IPS config:cmd=Write conditional config:: ips: 1, iscsi: 0, fcip: 1
iscsi-intf-vsan: 0, ips_lc: 1
```

Workaround: This issue is resolved.

- CSCtz73136

  Symptom: The following exceptions are logged in the module exception log of Cisco MDS 9000 Generation 4 modules:

  1. TBIRD_FWD_IAF_ACL_PIORD_LSB_ECC_ERR
  2. TBIRD_FWD_IAF_ACL_BANK0_LSB_ECC_ERR
  3. TBIRD_FWD_IAF_ACL_BANK1_LSB_ECC_ERR
  4. TBIRD_FWD_IAF_FIB_PIORD_LSB_ECC_ERR
  5. TBIRD_FWD_IAF_FIB_BANK0_LSB_ECC_ERR
  6. TBIRD_FWD_IAF_FIB_BANK1_LSB_ECC_ERR
  7. TBIRD_FWD_ETI_SPANS_PIORD_LSB_ECC_ERR
  8. TBIRD_FWD_ETI_SPANS_BANK0_LSB_ECC_ERR
  9. TBIRD_FWD_ETI_SPANS_BANK1_LSB_ECC_ERR

  The count of relevant errors per module (from the last time counters were cleared) can be seen by the following command:

  ```
  switch# show hardware internal errors all | inc "LSB_ECC| in module"
  ```

  If TACACS accounting is enabled, the following messages will be in the syslog:

  ```
  %TACACS-3-TACACS_ERROR_MESSAGE: All servers failed to respond
  %AAA-1-AAA_SESSION_LIMIT_REJECT: aaa request rejected as maximum aaa sessions are in
  progress
  ```

  This symptom occurs only on the Cisco MDS 9000 32-port 8-Gbps Advanced Fibre Channel Switching Module (DS-X9232-256K9) and the Cisco MDS 9000 48-port 8-Gbps Advanced Fibre Channel Switching Module (DS-X9248-256K9).

  The main cause of the issue is the exceptions generated on the module. These exceptions do not impact operations. However, the unthrottled notification exceptions are not desirable, and might cause switch resources to be overwhelmed. These notifications should be disabled until it is possible to upgrade to software where this issue is fixed.

  Workaround: This issue is resolved.

- CSCtz82290

  Symptom: An HDS AMS Truecopy path failure occurs in a topology with an HDS AMS initiator and target, and a Cisco MDS 9509 switch with a MSM-18/4 module and a Cisco MDS 9222i switch. IVR NAT is enabled with both devices in an IVR zone. The path between the initiator and target is active after the IVR zone set is enabled, but after the FCIP link goes down and then up, the Truecopy path stays offline unless a manual recovery is initiated. This problem does not occur without IVR.

  Workaround: This issue is resolved.

- CSCtz83956

Symptom: On an Cisco MDS 9513 switch, SCSI traffic sent from a LUN to a device configured for IVR or FC Redirect gets dropped.

This symptom occurs when the LUN numbers end with 0x2x, 0x22, or 0x81.

Workaround: This issue is resolved.

- CSCua04249

  Symptom: A FICON tape acceleration (FTA) control message that was received out of sequence caused the MSM-18/4 module to fail. This symptom occurred when FTA was enabled for read acceleration.

  Workaround: This issue is resolved.

- CSCua15818

  Symptom: Following an IVR zone set activation, a Cisco MDS 9148 switch loses connectivity within a VSAN.

  Workaround: This issue is resolved.

- CSCua47533

  Symptom: When FTA is disabled, a module reloads due to a null device entry.

  Workaround: This issue is resolved.

- CSCua61044

  Symptom: A device that is attached to a Cisco MDS 9000 48-port 8-Gbps Advanced Fibre Channel Switching Module (DS-X9248-256K9) or a Cisco MDS 9000 32-port 8-Gbps Advanced Fibre Channel Switching Module (DS-X9232-256K9) is not able to communicate with other devices.

  This symptom occurs only when a port on the DS-X9248-256K9 or DS-X9232-256K9 module is zoned to more than 146 unique devices.

  The following errors can be seen in the log of the DS-X9248-256K9 or DS-X9232-256K9 module:

```
switch# show process acltcam internal errors
  1) Event:E_DEBUG, length:84, at 359632 usecs after Tue Jun 19 23:34:44 2012
    [109] Program rqst sync failed. Fwd-eng:0(IN) ifIndex: 0x1104000, status:
0x404e0005
  2) Event:E_DEBUG, length:65, at 359603 usecs after Tue Jun 19 23:34:44 2012
    [112] Failed: tcamwrapv2_tcam_ssram_write, 155 entries, errno: 28
```

  Workaround: This issue is resolved.

- CSCtr20364

  Symptom: An RSCN is not sent to zone members in the IVR remote VSAN when the physical interface goes down.

  This symptom occurs when the devices are in an IVR zone. An RSCN is sent to local IVR VSAN zone members, but not to remote IVR VSAN zone members.

  Workaround: This issue is resolved.

- CSCtr41519

  Symptom: An ISSU might fail with the following message:

```
%MODULE-2-LCM_UPGRADE_READY_GENERAL_FAIL:
Upgrade ready message fails SAP Zone server
```

  This symptom occurs when suspended VSANs trigger it.

  Workaround: This issue is resolved.

- CSCua84273

  Symptom: A replaced smart card configuration is not persistent following a switch reload.

  Workaround: This issue is resolved.

- CSCub11370

  Symptom: A Cisco MDS 9124 switch incorrectly indicates that the TCAM is full when it is not. The symptom occurs when a Cisco MDS 9124 switch is in NPV mode and an NPIV switch is connected to it with PortChannels. If the NPIV mode switch reloads, the TCAM member table counter is not decreased.

  Workaround: This issue is resolved.

- CSCtr55608

  Symptom: Following the insertion of the 32-port 8-Gbps Advanced Fibre Channel switching module (DSX9232-256K9), the following syslog message is displayed:

  ```
  2011 Jul 16 05:35:00 emc-9513-II %SYSMGR-STANDBY-3-UNACCEPTABLE_WAIT: Service "r
  es_mgr", no response from System Manager after 10 seconds. Terminating.
  ```

  This issue might be seen if you enter the **no install feature-set fcoe** command, power down the 32-port 8-Gbps Advanced Fibre Channel switching module, and then insert the module again, which causes the **install feature-set fcoe** command to execute.

  Workaround: This issue is resolved.

- CSCtr83189

  Symptom: The Cisco MDS IOA feature fails when IOA flows frequently flap due to logout and to tape sessions that are cleaned up on the host and target IOA nodes.

  Workaround: This issue is resolved.

- CSCtr92846

  Symptom: An SME cluster with a single node goes offline after an upgrade from Cisco SAN-OS Release 3.3(1c) to Cisco NX-OS Release 4.2(7d).

  Workaround: This issue is resolved.

- CSCts16956

  Symptom: SANTap PLOGI ELS_Capture ACL is not programmed for SANTap VT/VI

  This symptom might occur when the AVT zone is large (over 50 members). The PLOGI LS_ACC can be dropped and not sent back to the EMC Recover Point Appliance (RPA).

  By programming in this new ACL entry, the LS_ACC will be captured by the supervisor module and delayed until the ACL programming is complete.

  The following drop counters will increment when this occurs:

  ```
  switch# show hardware internal fwd-ingress 0 error-statistics

  * ------------------------------------------------------------------------------
  * Global Error Statistics for device Tuscany-fwd
  * dev inst: 0, port(s): 1-22
  *
   ADDRESS     STAT                                                  COUNT
  __________ ________                                          ____________________
  0x00002d5c AD_ADJ_PKT_DROP_FCNT                                                0xxx

  Mapping for adj mem stats:
  ...
  0x40 - acl_default_no_match_drop
  ```

```
...
-------          -----                     ------
Address          Bytes                     Frames
-------          -----                     ------
...
 0040            00000000000016ac          0000000000000029
```

Workaround: This issue is resolved.

- CSCts71286

  Symptom: An AAA authentication error occurs.

```
switch(config)# aaa group server ldap ldap-group
switch(config)# aaa authentication login default group ldap-group
too big pss key or value size could not update aaa configuration
switch(config)#
```

  This symptom might be seen on a switch that is running Cisco NX-OS Release 5.x software or a later release, and a downgrade from Cisco NX-OS Release 5.1(x) or a later release occurs.

  Workaround: This issue is resolved.

- CSCts89154

  Symptom: The startup configuration does not sync up with the running configuration even after executing a **copy running-config startup-config** command. Additional interfaces appear in the startup configuration, even when the module does not have those ports present. For instance, for a module with 12 ports, such as the Cisco MDS 9000 12-port 4-Gbps Fibre Channel Switching Module (DS-X9112), the startup configuration shows that interfaces 13 through 24 also are present.

  Workaround: This issue is resolved.

- CSCtu07107

  Symptom: An interface fails with “Hardware Failure” and the exception log contains the error “RXF NP fifo overflow.”

```
switch# show int fc12/7
fc12/7 is down (Hardware failure)

switch# show logging log
%MODULE-2-MOD_SOMEPORTS_FAILED: Module x (serial: JAFxxxxxxx) reported failure
on ports x/8-x/8 (Fibre Channel) due to FC MAC Experienced an error in device
118 (error 0xc760020a)

switch# show module internal exceptionlog
 ********* Exception info for module x ********
exception information --- exception instance 1 ----
Module Slot Number: x
Device Id         : 118
Device Name       : Aakash
Device Errorcode  : 0xc760020a
Device ID         : 118 (0x76)
Device Instance   : 00 (0x00)
Dev Type (HW/SW)  : 02 (0x02)
ErrNum (devInfo)  : 10 (0x0a)
System Errorcode  : 0x40420010 FC MAC Experienced an error
Error Type        : Minor error
PhyPortLayer      : Fibre Channel
Port(s) Affected  : 8
Error Description : RXF NP fifo overflow, ref port 7
DSAP              : 0 (0x0)
UUID              : 543 (0x21f)
```

This symptom occurs only on the following Generation 3 modules:

- Cisco MDS 9000 24-Port 8-Gbps Fibre Channel Switching Module (DS-X9224-96K9)
- Cisco MDS 9000 48-Port 8-Gbps Fibre Channel Switching Module (DS-X9248-96K9)
- Cisco MDS 9000 4/44-Port Host-Optimized 8-Gbps Fibre Channel Switching Module (DS-X9248-48K9)

Workaround: This issue is resolved.

- CSCtu13569

  Symptom: The following truncated syslog message is printed when a 48-port 8-Gbps Advanced Fibre Channel module (DS-X9248-256K9) is inserted into a Cisco MDS 9000 switch chassis with a fabric 2 module.

  ```
  2011 Oct 31 10:28:22 MDS-FABRIC-B %XBAR-2-INCOMPATIBLE_CONFIG: Linecard in slot 3 is
  not supported with current switch fabric mode. Please upgrade to either DS-13SLT-FAB2
  or DS-13SLT-FAB3 switch fabricmodules in the case of 9513 chassis to supportthe
  linecard  and reload the switch. In the case of9506/9509 please re
  ```

  Workaround: This issue is resolved.

- CSCtw60823

  Symptom: When the configuration was copied using SNMP, the file transfer indicated it was complete but it was not. Subsequent attempts using SNMP to execute the **copy running-config startup config** command or to transfer the startup configuration using TFTP failed with the following message:

  ```
  "snmpd: another copy is in progress: Only one operation allowed at any one instance."
  ```

  This symptom occurs when you attempt to save the running-configuration to the startup-configuration through SNMP using Device Manager or Cisco Fabric Manager.

  Workaround: This issue is resolved.

- CSCtx02571

  Symptom: When a device alias is renamed and committed, the renamed entry appears in the device alias database and propagates to the active zone set, however, it does not propagate to the full zone set. If the running configuration is copied to the startup configuration, the old name still exists in the startup configuration.

  This symptom occurs regardless of basic or enhanced zoning, IVR, or non-IVR fabrics.

  Workaround: This issue is resolved.

- CSCtx17833

  Symptom: The TSM application that runs through the Storage Media Encryption (SME) feature on a Cisco MDS 9000 switch reports the following error message:

  ```
  ANR8311E An I/O error occurred while accessing drive DRIVEx (/dev/rmtx) for READ
  operation, errno = 78
  ```

  This error is a result of the Cisco MDS 9000 switch dropping a small number of SCSI data frames at the very end of a large read exchange. This symptom might be seen when the TSM server HBA is connected to the Cisco MDS 9000 switch at a speed of 2 Gbps.

  Workaround: This issue is resolved.

- CSCtx35664

Symptom: Device Manager does not show the power supply information correctly. Even if you make a change in redundant or combined mode, Device Manager shows the lowest value under capacity when you have two different power supplies.

Workaround: This issue is resolved.

- CSCtx77816

  Symptom: When a switch is upgraded from a lower software version to a higher version and PMON policies are configured, if there are counter differences in these software versions, the PMON policy cannot be removed from the higher version.

  This symptom occurs only when PMON policies are configured before the upgrade and extra counters are present in the upgraded version.

  Workaround: This issue is resolved.

- CSCty01555

  Symptom: Entering the **clear ntp session** command causes NTP to fail.

  This symptom occurs when there is a NTP CFS lock held by the switch.

  Workaround: This issue is resolved.

- CSCty01609

  Symptom: The standby supervisor remains in a powered-up state and not in HA standby even though a process is failing.

  Workaround: This issue is resolved.

- CSCty13815

  Symptom: Cisco MDS Storage Media Encryption (SME) will not function with an RSA key length of less than 1024 in Cisco NX-OS Release 5.2(1) and later releases.

  Workaround: This issue is resolved.

- CSCty30802

  Symptom: IVR per VSAN state information is missing local VSAN information.

  Workaround: This issue is resolved.

- CSCty33006

  Symptom: The fabric name that is configured in Cisco MDS SME does not match the fabric name in Cisco DCNM-SAN and there is no meaningful message about the mismatch.

  Workaround: This issue is resolved.

- CSCty57144

  Symptom: The management interface on a Cisco MDS 9148 switch is 10/half after the switch reloads.

  Workaround: This issue is resolved.

- CSCty80115

  Symptom: When a local node leaves a Cisco IOA cluster, a message needs to be displayed that provides the reason the node left.

  Workaround: This issue is resolved.

- CSCty97827

  Symptom: Host-to-target connectivity across multihop-connected switches is lost. The fc ping fails between devices through a PortChannel.

This issue is extremely rare. The conditions for this issue may be created after a nondisruptive upgrade to Cisco NX-OS Release 5.2(x). However, service disruption might not appear immediately on the affected PortChannel. The next time one or more members of the PortChannel flap, traffic loss could occur.

To verify if you have the potential to experience this issue, enter the commands shown in the following examples:

```
switch# show port-channel internal info interface port-channel 3

port-channel 3
channel     : 3   <<< channel_id
bundle      : 10  <<< normally, bundle_id = channel_id - 1
ifindex     : 0x4000002
pcport mode : 67108866
admin mode  : on
oper mode   : on
[...]

switch # show system internal fcfwd pcmap
port-channel 3:
    IfIndex is 0x04000002        <<< last 3 nibbles
    Bundle-Index is 0x0000000a   <<< last 3 nibbles are not equal
[...]
```

Regardless of the last three nibbles of the preceding indexes, this issue has been hit if the following output contains “pcm_reserv_bundle_id:Conflict,rsv a new one...”

```
switch# show port-channel internal event-history port-channel 1
29) Event: E_DEBUG at 487974 usecs after Thu Mar 22 19:44:26 2012
pcm_reserve_bundle_id:Conflict,rsv a new one.req_bundle=0x0,resp_bundle=0x1
```

Workaround: This issue is resolved.

- CSCtz04489

  Symptom: Cisco IOA issues the following messages:

  ```
  %LIBBASE_SVC-5-IT_NEXUS_FAILURE: IT-NEXUS (iwwn, twwn). IT-NEXUS on ioa4/1
  vi-vt (viwwn, vtwwn) bind failure. Reason: : 0x46
  %LIBBASE_SVC-5-IT_NEXUS_FAILURE: IT-NEXUS (iwwn, twwn). IT-NEXUS on ioa2/1
  vi-vt (viwwn, vtwwn) bind failure. Reason: : 0x26
  ```

  The reason text is not provided and the reason codes of 0x46 and 0x26 are not defined.

  Workaround: This issue is resolved.

- CSCtz13890

  Symptom: The size of the bootflash on a Cisco MDS 9222i switch might be smaller than expected. The bootflash should be around 650 MB, but on some Cisco MDS 9222i switches the bootflash size is 325 MB.

  Workaround: This issue is resolved.

- CSCtz15659

  Symptom: An ISSU upgrade fails with a core file for an FC Redirect process.

  ```
  switch# show cores

  Module-num       Instance-num      Process-name     PID Core-create-time
  ----------       ------------      ------------     --- ----------------
  8                1                fc-redirect      3097     Apr 4 12:59
  ```

This symptom occurred on a Cisco MDS 9513 switch with Cisco NX-OS Release 4.2(7a) that was upgrading to Cisco NX-OS Release 5.0(4d).

Workaround: This issue is resolved.

- CSCtz23936

  Symptom: Following an upgrade from Cisco NX-OS Release 3.3(x) to Release 4.2(x), IVR over FCIP caused an ENTERPRISE_PKG license to be checked out. Before the upgrade, IVR was using the SAN_EXTN_OVER_IP_IPS2 license. The ENTERPRISE_PKG license should not have been checked out as the SAN_EXTN_OVER_IP_IPS2 was still present.

  Workaround: This issue is resolved.

- CSCtz25933

  Symptom: Some onboard logging statistics are not updated as frequently as required. These statistics are used only for debugging limited types of problems.

  This symptom might be seen only on the 32-port 8-Gbps Advanced Fibre Channel module (DS-X9232-256K9) and the 48-port 8-Gbps Advanced Fibre Channel module (DS-X9248-256K9).

  Workaround: This issue is resolved.

- CSCtz44601

  Symptom: A username cannot be deleted.

  Workaround: This issue is resolved.

- CSCtz56349

  Symptom: A Fibre Channel interface is down. It is error-disabled because the port reinitialization limit has been reached.

  This symptom occurs when the module rootfs (/dev/root) is full, and the module FIB VmSize is larger than 15000 KB.

  First trigger is the module rootfs (/dev/root) is full.

```
switch# attach module x
module-4# show system internal flash
Filesystem           1K-blocks      Used Available Use% Mounted on
rootfs                   95195     95195         0 100% /
/dev/root                95195     95195         0 100% /

switch# attach module x
module-4# show process memusage |include "VmSize|fib"
Name            |PID     | VmSize  | VmData  |  VmStk  |  VmExe  |  VmLib  |
fib             |   1647 |  10192 k|   2548 k|     84 k|    288 k|   4808 k|
```

  The number in the VmSize column should not exceed 15000 KB.

  Workaround: This issue is resolved.

- CSCtz69973

  Symptom: A Cisco Fabric Services (CFS) process fails when a CFS application deregisters itself and a timeout occurs. The following messages are displayed:

```
%FSCM-2-FABRIC_START_CFG_MGR_PROGRAM_EXIT: Fabric Start Cfg Mgr daemon exiting: could
not register
with CFS
%SYSMGR-3-SERVICE_TERMINATED: Service "fscm" (PID 3704) has finished with error code
SYSMGR_EXITCODE_SYSERR (1).
```

```
%SYSMGR-STANDBY-5-CFGWRITE_STARTED: Configuration copy started (PID 2589).
%RADIUS-3-RADIUS_ERROR_MESSAGE: could not register with cfs: 0x80b3003e
%SYSMGR-2-SERVICE_CRASHED: Service "cfs" (PID 2883) hasn't caught signal 11 (core will
be saved).
```

Workaround: This issue is resolved.

- CSCtz85952

  Symptom: An F port interface goes down and will not come back up. The following error message is displayed:

  ```
  Link failure Link Reset failed nonempty recv queue
  ```

  This issue only affects interfaces on the Cisco MDS 9000 48-port 8-Gbps Advanced Fibre Channel Switching Module (DS-X9248-256K9) or the Cisco MDS 9000 32-port 8-Gbps Advanced Fibre Channel Switching Module (DS-X9232-256K9). It is triggered by shutting the last member (or the interface itself) of a downstream next-hop PortChannel while high rates of traffic are flowing from the edge port into the PortChannel.

  This issue cannot be cleared by shutting and not shutting the affected interface. It can be identified for an affected interface fc x/y with the following command:

  ```
  switch# attach module {x}
  module-x# show hardware internal credit-info port {y}
  Buffers are all used. (Configued-0x20, used = 0x26)
  module-x# exit
  ```

  The number of buffers used is greater than those configured.

  Workaround: This issue is resolved.

- CSCtz99466

  Symptom: The FSCM process exits without deregistering from Cisco Fabric Services (CFS). As a result, the following CFS events occur:

  ```
  Wed May  2 15:44:41 2012 :
  MTS send failed, retval -1, errno 32 [Broken pipe]
                  Dest sap 139, opcode 8465
  ```

  This symptom occurs after the FSCM process exits or fails or both four times and is not restarted due to a sysmgr policy.

  Workaround: This issue is resolved.

- CSCua02159

  Symptom: Hosts that are zoned by a device alias cannot see storage.

  This symptom occurs in an active zone set, and there is no FCID next to the device alias; however, the FCID is in the FCNS database.

  ```
  switch# show zoneset active
    zone name myserver_hba0-mystorage_8D0 vsan 10
    * fcid 0x363d00 [device-alias myserver_hba0]
      device-alias mystorage_8D0
  switch# show fcns database
  VSAN 10:
  --------------------------------------------------------------------------
  FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
  --------------------------------------------------------------------------
  0x110000    N     50:00:11:22:33:44:55:66                 scsi-fcp:target
                    [mystorage_8D0]
  ```

There are duplicate pPWWNs.

```
switch# show zone internal ddas-table
Device Alias Database State: 1
Device Alias Mode: enhanced
--------------------------------------------------------------------------------
Device Alias Name                                        PWWN
--------------------------------------------------------------------------------
mystorage_8DA                                          50:00:11:22:33:44:55:66
mystorage_8D0                                          50:00:11:22:33:44:55:66
```

Workaround: This issue is resolved.

- CSCua34425

  Symptom: The Cisco MDS 9513 multilayer switch that is running Cisco NX-OS Release 5.0(1a) includes a version of OpenSSL that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

  CVE-2012-0814

  This bug was opened to address the potential impact on this product.

  This symptom occurs on a device with a default configuration.

  Additional details about the vulnerabilities listed above can be found at http://cve.mitre.org/cve/cve.html

  Workaround: This issue is resolved.

- CSCua37931

  Symptom: The **show tech-support** command does not work properly for users with a role other than network-admin. Sections of the command that require access to modules will time out and be missing from the output.

  The symptom occurs because non-network-admin users are not being permitted to attach to a module. The following error messages are displayed when such a user enters this command:

  ```
  switch# attach module 1
    This command can only be run by the network admin
  ```

  If a role is created and permit **attach** is added to the role, the command will fail with the following error message:

  ```
  switch# attach module 1
    % Permission denied for the role
  ```

  This issue affects any user with a role other than network-admin.

  Workaround: This issue is resolved.

- CSCua72788

  Symptom: The IKE service might fail and produce a core dump on a Cisco MDS 9509 switch that is configured for IPsec with IKE. The failure occurs during a IKE rekey operation.

  This symptom occurs on a Cisco MDS 9509 that is running Cisco NX-OS Release 4.2(1b).

  Workaround: This issue is resolved.

- CSCub09763

  Symptom: When hosts are added to the FE VSAN, the MSM-18/4 module (DS-X9304-18K9) that is running SANTap might experience a ps_stap core.

  This symptom occurs when hidden LUNs are installed and the number of LUNs per host exceeds the maximum limit. The following messages might be seen before the core:

```
2012 Jul 12 10:31:56 MDS03 %SANTAP-SLOT3-4-ST_NEAR_MAX_LUNS_PER_HOST: Warning:
Approaching
MAX_LUNS_PER_HOST(256) limit for Host 1:2:3:4:5:6:7:8, DVT
1:2:3:4:5:6:7:8. Existing num luns 230
2012 Jul 12 10:31:56 MDS03 %SANTAP-SLOT3-4-ST_NEAR_MAX_LUNS_PER_HOST: Warning:
Approaching
MAX_LUNS_PER_HOST(256) limit for Host 1:2:3:4:5:6:7:8, DVT
1:2:3:4:5:6:7:8. Existing num luns 230
2012 Jul 12 10:31:57 MDS03 %SANTAP-SLOT3-4-ST_NEAR_MAX_LUNS_PER_HOST: Warning:
Approaching
2012 Jul 12 10:31:59 MDS03 %SANTAP-SLOT3-2-ST_MAX_LUNS_PER_HOST_REACHED:
MAX_LUNS_PER_HOST(256) limit reached for Host 1:2:3:4:5:6:7:8, DVT
1:2:3:4:5:6:7:8. Cannot Install Lun 0xyyyy
2012 Jul 12 10:32:00 MDS03 %PROC_MGR-SLOT3-2-ERR_MSG: ERROR: PID xxxx (ps_stap)
killed
with signal (11)
```

Workaround: This issue is resolved.

- CSCub27133

  Symptom: Following an ISSU or ISSD, DMM is not configured on a a module where IPFC and DMM were previously configured.

  Workaround: This issue is resolved.

- CSCtr01652

  Symptom: The F port trunking and channeling between a Cisco MDS switch and a Cisco UCS server fails with the following error:

  ```
  %PORT-5-IF_PORT_QUIESCE_FAILED: Interface fcx/y port quiesce failed due to
  failure reason: Force Abort Due to Link Failure (NOS/LOS) (0x119)

  %PORT-5-IF_DOWN_OLS_RCVD: %$VSAN X%$ Interface fcx/y is down (OLS received)
  port-channel X <>
  ```

  Condition: Certain organizational unique identifiers (OUIs) are not being recognized as a result of which port channel fails.

  Workaround: This issue is resolved.

Note In Cisco MDS Release 5.2.6, these OUIs are added: 0x002a6a, 0x00defb, and 0x8c604f.

Open Caveats

- CSCtn72391

  Symptom: Following a switch reload or a software upgrade, the startup configuration occasionally does not display feature FCIP.

  Workaround: Once the switch is completely up, copy the running configuration to the startup configuration by entering the **copy running-config startup-config** command.

- CSCtr10877

  Symptom: Following an ISL flap that isolates some switches in the fabric (and the corresponding FCR peers) and then later merges them again, some FCR peers might get out of sync with the SSM switch FCR peer (that is, the FCR peer that owns a configuration) during the peer discovery phase. Consequently, some application flows might not come online, or might even get deleted.

Workaround: Enter the following supervisor commands on the problematic FCR peer, which will trigger this FCR peer to resync with the rest of the fabric, and force it to come out of the error state:

```
switch# test fc-redirect config sync-with-fabric
switch# test fc-redirect config sync-with-fabric all-peers
```

If more than one peer is affected by this issue, then additional steps are needed. If the application flows do not come online, then the application CLI commands need to be checked to verify that the flows did not get deleted. If they did, then the flows need to be recreated again through the application CLI command s or Cisco DCNM-SAN interface.

- CSCtw64713

  Symptom: Occasionally, a 10-G ISL between a 32-port 8-Gbps Advanced Fibre Channel Switching Module (DS-X9232-256K9) or a 48-port 8-Gbps Advanced Fibre Channel Switching Module (DS-X9248-256K9) and an older generation Cisco MDS 9000 module can take a long time to come up. The link can go into an error-disabled state.

  Workaround: None.

- CSCty59570

  Symptom: After replacing a smart card that reached the maximum number of shares (16), the new smart card gets stuck in the initializing state.

  Workaround: None.

- CSCty68838

  Symptom: Periodic FCIP port flaps might occur when Tape Acceleration and IP compression are enabled and the MTU is configured at 9000. This situation might lead to a failure of an IPS core.

  This symptom might be seen when the following configuration is applied to an FCIP tunnel:

  - Tape Acceleration (TA) is enabled.
  - Write Acceleration (required for TA) is enabled.
  - IP compression in enabled.
  - The MTU size is 9000.

  Workaround:

  This issue does not occur if TA is not configured and other parameters remain the same.

  This issue does not occur if the MTU size of up to 2500 is configured and other parameters remain the same.

- CSCty82906

  Symptom: On a Windows XP system, master key rekey cannot detect a smart card and displays the following message:

  ```
  Exception reading smartcard:CKR_OPERATION_NOT_INITIALIZED
  ```

  Workaround: None.

- CSCua12379

  Symptom: On a Windows 7 32-bit system, there is an issue with the Java version detect plugin. In addition, the pkcs11wrapper.dll file is not copied over correctly.

  Workaround: None.

- CSCub47799

  Symptom: Zone crash or switch reload occurs after renaming an enhanced device-alias.

Condition: This issue applies to the following NX-OS versions or platform combinations only:

- The Cisco MDS switches running MDS NX-OS Release 5.2(6), 5.2(6a), 5.2(6b), 5.2(8), 5.2(8a), or 6.2(1).
- The Cisco Nexus 7000 switches running NX-OS version 6.1(3) or 6.1(4).

In addition, the following conditions must be true:

- Device-alias is set to enhanced mode by using the **device-alias mode enhanced** command.
- Multiple commands are performed on the same device-alias before a commit and one of which is the **rename** command.

Note This issue occurs in both zone mode basic and zone mode enhanced.

Workaround: To avoided this issue group the device-alias commands of the same type together and commit the changes before starting the next type. For example, use the **device-alias commit** command after each and every same type of device-alias action. See the examples below.

Example 1

The following example shows how to delete the Alias2 and rename Alias1 to Alias2:

```
device-alias rename Alias1 temp_Alias1
device-alias rename Alias2 temp_Alias2
device-alias commit
```

Use the **show device-alias session status** command to verify the device-alias session status.

```
device-alias rename temp_Alias1 Alias2
device-alias commit
```

Use the **show device-alias session status** command to verify the device-alias session status.

If you do not need temp_Alias2, use following commands:

```
device-alias delete temp_Alias2
device-alias commit
```

The following example shows how to delete the Alias2 and rename Alias1 to Alias2:

Example 2

```
device-alias delete Alias2
device-alias commit
```

Use the **show device-alias session status** command to verify the device-alias session status.

```
device-alias rename Alias1 Alias2
device-alias commit
```

Use the **show device-alias session status** command to verify the device-alias session status.

Note You can use multiple device-alias commands of the same type such as **delete**, **rename**, and **add** in the same batch if the names of all the device-alias that areaffected are unique.

- CSCub51064

  Symptom: An ISSU from Cisco MDS Release 4.2(7dE5) to Release 5.2(6) fails when the number of IOA tape acceleration flows exceeds 511.

This issue might be seen on an Cisco MDS 9000 Series switch with the MDS 9000 18/4-port Multiservice (MSM-18/4) module.

Workaround: None.

- CSCuc35483

  Symptom: Activation of a zone set in a VSAN in interop mode 1, fails with the following error messages:

  ```
  %ZONE-2-ZS_CHANGE_ACTIVATION_FAILED_RESN_DOM: %$VSAN <vsan>%$ Activation failed
  : reason Invalid zonset format domain <dom>
  %ZONE-2-ZS_CHANGE_SFC_FAILED: %$VSAN <vsan>%$ SFC failed : domain <dom> returns
  INVALID_ZSET_FORMAT
  ```

  The failure occurs only if the following conditions exist:

  - Zone set activation occurs from a Cisco MDS 9000 switch.
  - The switch is running Cisco NX-OS Release 5.2(6) or Release 5.2(6a).
  - The VSAN in question is running in interop mode 1.
  - McData switches are present in the VSAN that is in interop mode 1.

  Workaround:

  There are two methods for working around this issue:

  - Leave the VSAN in interop mode 1 and do all zoning from the McData side. This method is completely nondisruptive.
  - Convert VSAN to interop 4. This method is disruptive to the entire VSAN becuase it needs to be suspended and the fcdomain domains need to be adjusted to be in the range of 1 to 31.

- CSCuc84790

  Symptom: Following an upgrade to NX-OS Release 5.2(6) or Release 5.2(6a), FCIP interfaces are down and the following message appears:

  ```
  fcip1 is down (Tunnel port src interface unbound)
  ```

  The licenses for all SAN_EXTN_OVER_IP packages in the grace period might be unnecessarily checked out.The inter-VSAN routing (IVR) process is using those licenses.

  ```
  switch# show ivr

  License status
  ----------------
  IVR is running based on the following license(s)
  SAN_EXTN_OVER_IP
  SAN_EXTN_OVER_IP_IPS2
  SAN_EXTN_OVER_IP_IPS4
  SAN_EXTN_OVER_IP_9216i
  SAN_EXTN_OVER_IP_18_4
  SAN_EXTN_OVER_IP_SSN16
  ```

  Conditions: This symptom might be seen when IVR is running over FCIP.

  Workaround: To work aorund this issue, follow these steps:

  1. Enter the **show license usage** *license package name* command to identify the applications that are using the license. For example:

  ```
  switch# show license usage SAN_EXTN_OVER_IP_18_4
  Application
  --------------------------------------------------------------------------------
  ```

```
IVR_FCIP
--------------------------------------------------------------------------------
```

2. Back up the FCIP configuration and other applications from the running configuration on the switch.
3. Disable the features in use by the license. This action is disruptive to any non-FCIP IVR traffic.

```
switch# no feature fcip
switch# no feature IVR
```

4. Copy the license files off the switch as follows:

```
switch# copy licenses bootflash:lic-backup.tar
switch# copy bootflash:lic-backup.tar tftp://xxx.xxx.xxx.xxx
```

5. Enter the **clear license** command to clear the license.
6. Reinstall the license files.
7. Enable FCIP and reconfigure the switch.
8. Enable IVR and reconfigure the switch.

- CSCuf31077

  Symptom: Ports on the 24-port, 48-port, or 4/44-port 8-Gbps Fibre Channel switching modules go into a suspended state and packets cannot egress or ingress on the port. This issue can occur on Cisco MDS 9500 Series Directors and Cisco MDS 92221 switches when any of the following modules are installed:

  – 24-port 8-Gbps Fibre Channel switching module (DS-X9224-96K9)
  – 48-port 8-Gbps Fibre Channel switching module (DS-X9248-96K9)
  – 4/44-port Host Optimized 8-Gbps Fibre Channel switching module (DS-X9248-48K9)

  Conditions: This issue occurs after a nondisruptive upgrade to Cisco NX-OS Release 5.2(6x) or Release 5.2(8), and a link flap occurs on the ports.

  Workaround: To work around this issue, do one of the following:

  1. To temporarily recover a port in this state, enter the **shut** command followed by the **no shut** command on the port. A port that is recovered in this way can fail again.
  2. To permanently work around this issue, reload the affected 24-port, 48-port, or 4/44-port 8-Gbps Fibre Channel switching module. If the switch contains primarily these modules, then reload the entire switch. Following the reload, the issue will not reoccur.
  3. Downgrade or upgrade the Cisco NX-OS software to a release that is not affected by this bug. If a port is in this suspended state at the time of the upgrade or downgrade, the upgrade or downgrade does not automatically recover the port. Enter the **shut** command followed by the n**o shut** command on the port after the upgrade or downgrade is complete to recover the port.

  Further Problem Description: The main indications of a port exhibiting this issue are the following:

  – The interface is up, there is an F port, there are zero frames per second in and out, there are output discards, and all B2B credits are remaining.
  – Logging onboard shows small numbers of OFFLINE and TIMEOUT drops that are incrementing.

- CSCtq88900

Symptom: In an SME or IOA deployment, if the number of H->T flows that are added exceeds 512, then subsequent disruptive platform events can leave an FCR unable to process interprocess (MTS) messages at a rate fast enough to support the scaled configuration. This situation can cause an MTS-buffers full condition in the FCR, which can result in unpredictable behavior. Some of the resulting errors may be unrecoverable, and may require a disruptive restart of the flows.

Workaround: Use CFS regions if a large number (greater than 512) of application flows need to be configured. CFS regions segment the FCR peer topology into manageable proportions.

- CSCtr50223

  Symptom: On the MDS 9513 switch, when an MSM-18/4 module boots up, it sends a request to the supervisor module to mount the modflash on the MSM-18/4 module. If there is a timeout or error in response, the following syslog message displays:

  ```
  2011 Jul 14 01:18:13 sw-dc5-br2-12 %LC_MNT_MGR-SLOT3-2-LC_MNT_MGR_ERROR: SUP mount
  failed. MTS receive timedout
  2011 Jul 14 01:19:06 sw-dc5-br2-12 %PROC_MGR-SLOT3-2-ERR_MSG: ERROR: PID 1144
  (lc_mnt_mgr) exited abnormally, exit status (0xa)
  2011 Jul 14 01:19:06 sw-dc5-br2-12 %MODULE-2-MOD_MINORSWFAIL: Module 3 (serial:
  JAE1141ZB43) reported a failure in service lc_mnt_mgr
  ```

  This issue might be seen when the supervisor module is unusually busy and cannot process the mount request from the MSM-18/4 module, or the actual mount command on the supervisor takes a long time.

  Workaround: Reload the MSM-18/4 module in the same slot/module where the modflash mount failed. A request will be sent to the supervisor to mount the modflash.

- CSCtx41288

  Symptom: The label for a smart card is not detected correctly.

  Workaround: None.

- CSCty82821

  Symptom: After creating an SME cluster, adding disks to a disk group, changing some disk states, and starting master key rekey, the key creation date is invalid.

  Workaround: None.

- CSCua61011

  Symptom: After creating an SME cluster in advanced mode, adding 500 disks to the disk group, exporting the keys, and importing the keys again, there is no scroll option in the import manage key window.

  Workaround: None.

- CSCub52623

  Symptom: On a Cisco MDS 9000 switch with the MSM-18/4 module that is running FC Redirect, host ports and destination ports become error-disabled after flapping. The logs show the following errors:

  ```
  switch(config-if)# sh int fc1/17 br

  --------------------------------------------------------------------------------
  Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                    Mode   Trunk                          Mode  Speed  Channel
                           Mode                                 (Gbps)
  --------------------------------------------------------------------------------
  fc1/17     1      FL     --      errDisabled      swl    --           --
  switch(config-if)#
  ```

```
switch(config)# ivr aam pre-deregister-check
switch(config)# show ivr aam pre-deregister-check

AAM pre-deregister check status
--------------------------
FAILURE

There are merged entries or AAM has not been enabled with the following switches:
  switch swwn 20:00:00:0d:ec:3e:f4:c0
```

Workaround : Disable IVR and AAM support on FCR and flap the ports:

```
switch (config)# no fc-redirect ivr-support enable
switch (config)# no ivr aam register
AAM is currently disabled. No change will be made.
switch (config)#
switch (config)# ivr commit
distribution not enabled
switch (config)# int fc1/17
switch (config-if)# shut
switch (config-if)# no shut
switch (config-if)# sh int fc1/17 br

--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                  Mode   Trunk                          Mode  Speed  Channel
                         Mode                           (Gbps)
--------------------------------------------------------------------------------
fc1/17     1      FL     --      up               swl    FL      2    --
switch (config-if)#
```

- CSCtz09820

  In Generation 4 modules, the following errors might be observed. They are not a cause for concern to the normal operation of the hardware. These errors are logged in the onboard persistent log and can be viewed by entering the **show logging onboard exception-log** command after attaching to the module.

  ```
  TBIRD_FWD_EBM_0_SER_PARITY_XXX  : Informational
  TBIRD_FWD_EBM_0_PACK0_EPR_DROP  : Informational
  TBIRD_FWD_EBM_1_PACK3_MISS_SOF  : Informational
  TBIRD_FWD_EBM_1_PACK0_MISS_EOP  : Informational
  TBIRD_FWD_EBM_1_PACK0_SF_TOO_SMALL : Informational
  ```

  These errors are reported when there are internal correctable conditions encountered during operation, and the corrective action is taken. They do not necessarily indicated a problem with the switch or module.

  The following error can occur in cases of corrupted frames in the ingress path (due to a bad cable or SFP). It does not necessarily indicated a problem with the switch hardware.

  ```
  THB_IPA_IPA0_INTR_FLD_ERR_FROM_MEM : Warning
  ```

  Workaround: None.

- CSCtz19169

  Symptom: After the primary KMC fails over to the secondary, KMC performance suffers. The system attempts to reacquire connectivity to the primary KMC for each operation, and the system waits for that attempt to time out before using the secondary KMC. Waiting for the timeout creates a significant delay for failed over operations, particularly when scaled.

  This symptom occurs when the primary KMC fails (because of loss of connectivity).

Workaround: Restore connectivity to the primary KMC.

- CSCtz40700

  Symptom: When a trunk link fails, the 1.3.6.1.4.1.9.9.289.1.3 trap has an incorrect link failure reason of “gracefully down.”

  This symptom might be seen only when a link failure occurs on a E, TE, or TF port.

  Workaround: Ignore the link down reason because the link down trap is valid.

- CSCtz40745

  Symptom: A “VSAN down” trap is sent for VSAN 4094 when a trunk port goes down because the VSAN is not configured on the trunk.

  This symptom might be seen only when a link down occurs on a E, TE, or TF port.

  Workaround: Ignore the trap.

- CSCua09712

  Symptom: Communication errors that occur during master key rekey are not handled gracefully.

  Workaround: None.

- CSCtz84847

  Symptom: When creating a cluster, key management servers are not listed in the drop-down list.

  Workaround: Manually enter the IP address of the server.

- CSCty47599

  Symptom: For a failed master key rekey, the master key shares were generated and updated in the CKMC.

  Workaround: None.

- CSCuh27347

  Symptom: During an In Service Software Upgrade (ISSU) or In Service Software Downgrade (ISSD), ports that are administratively up and also in the not-connected state get reinitialized.

  Condition: This issue affects all Cisco MDS dual-supervisor systems.

  Workaround: If starting an ISSU/ISSD from an affected version of Cisco MDS NX-OS software, ensure that all ports that are administratively up, but not connected, are shut down during the ISSU/ISSD.

  More Information: This might cause the Cisco MDs Generation 3 Fibre Channel switching modules to drop all outbound traffic with the OFFLINE and TIMEOUT errors. For more information, see CSCuf31077.

- CSCum30306

  Symptom: The security service crashes when configuring an SSH authentication key.

  Configuring SSH keys multiple times within 10 minutes results in a HAP reset that resets the active supervisor.

  Condition: This issue intermittently occurs when configuring an SSH authentication key.

  Workaround: To avoid the supervisor reset, do not configure more than 2 SSH keys per 10 minutes.

Related Documentation

The documentation set for NX-OS for the Cisco MDS 9000 Family includes the following documents. To find a document online, access the following web site:

http://www.cisco.com/en/US/products/ps5989/tsd_products_support_series_home.html

The documentation set for Cisco Fabric Manager appears in the *Cisco Fabric Manager Release Notes for Release 4.2(1)*, which is available from the following website:

http://www.cisco.com/en/US/products/ps10495/prod_release_notes_list.html

Release Notes

- *Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Releases*
- *Cisco MDS 9000 Family Release Notes for MDS SAN-OS Releases*
- *Cisco MDS 9000 Family Release Notes for Storage Services Interface Images*
- *Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images*

Regulatory Compliance and Safety Information

- *Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family*

Compatibility Information

- *Cisco Data Center Interoperability Support Matrix*
- *Cisco MDS 9000 NX-OS Hardware and Software Compatibility Information and Feature Lists*
- *Cisco MDS NX-OS Release Compatibility Matrix for Storage Service Interface Images*
- *Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide*
- *Cisco MDS NX-OS Release Compatibility Matrix for IBM SAN Volume Controller Software for Cisco MDS 9000*
- *Cisco MDS SAN-OS Release Compatibility Matrix for VERITAS Storage Foundation for Networks Software*

Hardware Installation

- *Cisco MDS 9500 Series Hardware Installation Guide*
- *Cisco MDS 9500 Series Supervisor-2A Tech Note*
- *Cisco MDS 9200 Series Hardware Installation Guide*
- *Cisco MDS 9100 Series Hardware Installation Guide*
- *Cisco MDS 9124 and Cisco MDS 9134 Multilayer Fabric Switch Quick Start Guide*

Software Installation and Upgrade

- *Cisco MDS 9000 NX-OS Software Upgrade and Downgrade Guide*
- *Cisco MDS 9000 Family Storage Services Interface Image Install and Upgrade Guide*
- *Cisco MDS 9000 Family Storage Services Module Software Installation and Upgrade Guide*

Cisco NX-OS

- *Cisco MDS 9000 Family NX-OS Licensing Guide*
- *Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide*
- *Cisco MDS 9000 Family NX-OS System Management Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Fabric Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Quality of Service Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Security Configuration Guide*
- *Cisco MDS 9000 Family NX-OS IP Services Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Intelligent Storage Services Configuration Guide*
- *Cisco MDS 9000 Family NX-OS High Availability and Redundancy Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Inter-VSAN Routing Configuration Guide*

Command-Line Interface

- *Cisco MDS 9000 Family Command Reference*

Intelligent Storage Networking Services Configuration Guides

- *Cisco MDS 9000 I/O Acceleration Configuration Guide*
- *Cisco MDS 9000 Family SANTap Deployment Guide*
- *Cisco MDS 9000 Family Data Mobility Manager Configuration Guide*
- *Cisco MDS 9000 Family Storage Media Encryption Configuration Guide*
- *Cisco MDS 9000 Family Secure Erase Configuration Guide*
- *Cisco MDS 9000 Family Cookbook for Cisco MDS SAN-OS*

Troubleshooting and Reference

- *Cisco NX-OS System Messages Reference*
- *Cisco MDS 9000 Family NX-OS Troubleshooting Guide*
- *Cisco MDS 9000 Family NX-OS MIB Quick Reference*
- *Cisco MDS 9000 Family NX-OS SMI-S Programming Reference*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2012–2014 Cisco Systems, Inc. All rights reserved.